Israel Public Policy Institute

HEINRICH BÖLL STIFTUNG

HEINRICH BÖLL STIFTUNG TEL AVIV

German-Israeli Tech Policy Dialog Program

Germany's Troubled Trajectory with Mass Surveillance and the European Search for Safeguards

Thorsten Wetzling

Rethinking Privacy and Mass Surveillance in the Information Age

Paper Series by the Israel Public Policy Institute and Heinrich-Böll-Stiftung

Germany's Troubled Trajectory with Mass Surveillance and the European Search for Safeguards

Author

Dr. Thorsten Wetzling

Project Lead

Heinrich Böll Foundation, Foreign and Security Policy Division, Berlin

Heinrich Böll Foundation Tel Aviv

Israel Public Policy Institute (IPPI)

Please cite as follows:

Wetzling, T. (2020). *Germany's Troubled Trajectory with Mass Surveillance and the European Search for Safeguards*. Paper Series "Rethinking Privacy and Mass Surveillance in the Information Age". Israel Public Policy Institute and Heinrich Böll Foundation

About the Project

The following paper has been commissioned by the Heinrich Böll Foundation and the Israel Public Policy Institute (IPPI) as part of the paper series "Rethinking Privacy and Mass Surveillance in the Information Age." Against the backdrop of the COVID-19 pandemic, this publication series has set out to examine the societal and political implications of the spillover of surveillance technologies from the security sphere into everyday life.

About the German-Israel Tech Policy Dialog Program

The paper series "Rethinking Privacy and Mass Surveillance in the Information Age" is part of the German-Israeli Tech Policy Dialog program of the Heinrich Böll Foundation and the Israel Public Policy Institute (IPPI). By facilitating a collaborative space for researchers and practitioners from politics, academia, tech and civil society, the program sets out to cultivate a community of committed professionals from both countries to deliberate the impact and governance of emerging technologies and to generate new actionable insights in support of democratic values.

Israel
Public Policy
Institute

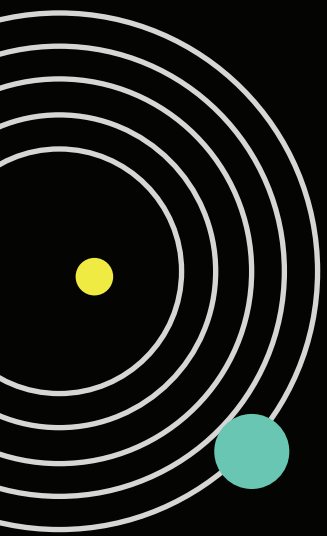
Israel Public Policy Institute (IPPI)

The Israel Public Policy Institute (IPPI) is an independent policy think-and-do-tank and a multi-stakeholder dialog platform at the intersection of society, technology and the environment. Through its research activities, knowledge sharing, networking and public outreach, IPPI contributes to the innovation of public policy with the goal of understanding, guiding, and advancing the transformation process of our societies towards a sustainable and democratic future. IPPI works with a global network of actors from government, academia, civil society, and the private sector to foster international and interdisciplinary cross-pollination of ideas and experiences.

HEINRICH
BÖLL
STIFTUNG

Heinrich Böll Foundation

The Heinrich Böll Foundation is an independent global think-and-do-tank for green visions. With its international network of 33 international offices, the foundation works with well over 100 project partners in more than 60 countries. The foundation's work in Israel focuses on fostering democracy, promoting environmental sustainability, advancing gender equality, and promoting dialog and exchange of knowledge between public policy experts and institutions from Israel and Germany.



Contents

Executive Summary

The landscape of digital communications and the evolution of surveillance technology is developing at unprecedented speed. As governments and industry actors debate new joint ventures to harness the potential of artificial intelligence in contexts of 5G and facial and biometric recognition systems and as cloud computing becomes ever more prevalent, so do the volume, variety and velocity of available data for government surveillance. These processes accelerate exponentially – not just in China but also in our democracies.

Governments serving open societies face immense challenges in coping with these new developments. For example, they need to engage much more in international cooperation as many threats, as well as supply chains for critical technology components, are transnational in nature. This may not be an easy transition for governments who still consider intelligence as the last bastion of national sovereignty. Given the enormous troves of data at their disposal, information overload remains a security risk, too. Yet, one must not overlook an equally severe and arguably even more pressing risk for our democracies, namely the erosion of fundamental rights and civil liberties. When the widespread acceleration in surveillance activity is not matched by a genuine evolution of adequate checks and balances, this can have far worse effects for the social fabric of our societies than the threats the surveillance is meant to address.

Current investments in advanced surveillance capabilities are driven by new technological possibilities. Yet, modern surveillance techniques struggle immensely to build human rights, democratic governance and ethics into their source code. In order to avoid dystopian realities, the legal frameworks and the oversight toolkit urgently need to catch-up and investment in AI and supervisory technology for oversight are overdue.

As this case study on Germany's recent troubled history with mass surveillance in the context of foreign intelligence collection shows, this is far easier to proclaim than to implement. It takes enormous strength by a persistent civil society and an independent judiciary to create positive change. While, obviously, there can be legitimate government interests in surveillance, the executive branch in Germany exploited accountability gaps and resisted effective democratic control for far too long. Now, in late 2020 the German parliament has a unique chance to adopt intelligence legislation that meets the long list of safeguards required not just by the German Constitutional Court but also by similar jurisprudence from the European Court of Justice. This process, I suspect, will be interesting to watch from abroad, too. This is because the question of how personal data can and will be protected against disproportionate interference by the state will remain a decisive question not just in transatlantic and EU-UK data transfers but also for democracies in general.

1. Introduction

Many democracies struggle to reconcile effective intelligence services with the need to invest in adequate safeguards and effective oversight. Some see it as a zero-sum process: Whatever a country might gain through robust surveillance reforms in terms of legality and legitimacy is lost from the vantage point of national security. Or, conversely, new investments in modern intelligence capacities will inevitably lead to a loss of fundamental freedoms.

While definitions of mass surveillance remain contested and vary significantly across democracies, a lot of ground has been covered in the seven years since the disclosures of Edward Snowden.

Personally, I find such views to be short-sighted. Liberal democracies should try to find the balance point that lies equidistant to these divergent positions. This requires an elaborate and inclusive adjustment process with several actors involved. It is a constant work in progress, but countries can invest in freedom without a loss to security and vice versa. Admittedly though, the devil is in the details. And this brings us to the focus of this paper: How has Germany steered the course when it comes to foreign intelligence collection by means of signals intelligence? Has it succeeded in using this key instrument of modern security provision without allowing disproportionate government access to private data?

While definitions of mass surveillance remain contested and vary significantly across democracies, a lot of ground has been covered in the seven years since the disclosures of Edward Snowden.

To answer this question, this paper sheds light on Germany's recent trajectory in regulating the foreign intelligence collection powers of the Federal Intelligence Service (Bundesnachrichtendienst, or BND). This has been a major bone of contention in German security politics throughout the past few years and given rise to major reforms. Germany's trajectory offers a unique tale of power, interests, and multi-level governance. It also includes a vibrant civil society that was not meant to have an impact. The analysis focuses on key stages in Germany's unique and troubled relationship with mass surveillance. The last segment discusses how the country might now set new standards and contribute to the necessary harmonization of adequate safeguards across Europe.

1.1. Mass Surveillance or Bulk Collection?

Before diving deeper into this, the reference object of the paper – mass surveillance – needs further unpacking. Governments prefer to use the terms "bulk interception" or "bulk collection." Are they euphemizing an ugly truth? This is best answered by examining both the definitions and the actual practices.

While definitions of mass surveillance remain contested and vary significantly across democracies, a lot of ground has been covered in the seven years since the disclosures of Edward Snowden. In order to understand this complex and technical matter, it helps to distinguish first between targeted and untargeted surveillance. According to the UK government, when intelligence agencies "acquire information in large volumes" to "generate intelligence about threats that cannot be acquired by more targeted means,"

→

they refer to "bulk data." While various methods may be used to acquire bulk data, they all share the common feature that the measure itself is not directed at a particular individual.

Reviewing the so-called bulk powers in an authoritative report, the UK's then Independent Reviewer of Terrorism Legislation warned that the use of bulk data may have serious adverse human rights implications given that they "involve potential access by the state to the data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime." Yet, he also cautioned against using the embattled term mass surveillance in contexts where a "legal system [...] incorporate(s) limitations and safeguards designed [...] to ensure that access to stores of sensitive data [...] is not given on an indiscriminate or unjustified basis."

What about Germany? Can one speak of justified and systematic government access to troves of data in the German context? Or is it more fitting to speak of mass surveillance? To answer this, one needs to carefully analyze the legal safeguards and oversight regime as they are written into the country's intelligence legislation but also how the formal oversight mandate is being practiced on the ground. In this paper, I will focus on the most significant signals intelligence practice of Germany's foreign intelligence service, the Bundesnachrichtendienst. By this, I mean its surveillance of international communications data that have both their origin and destination outside of Germany (Ausland-Ausland Fernmeldeaufklärung). Therein alone lies a unique governance tale that, I hope, will be of interest to foreign readers.

Having said this, I need to introduce an important caveat: With its focus on foreign intelligence collection, this paper will not have room to discuss other important intelligence methods available to the BND and Germany's other two intelligence services at the federal level, the Federal Office for the Protection of the Constitution (Bundesverfassungsschutz, BfV) and the Military Counterintelligence Service (Militärischer Abschirmdienst, MAD). What is more, the paper will discuss neither the intelligence-led policing practices by Germany's Federal Criminal Police Office (Bundeskriminalamt, BKA) nor the signals intelligence and other cyber operations conducted by special forces within the German military.

1.2. What is the Fuss about Signals Intelligence and Who is Interested?

Most governments in liberal democracies not only have an interest but are also constitutionally obliged to protect their citizens from harm. This requires them to keep abreast of a wide range of possible threats. To do this, they may rely on information and tip-offs from international partners. However, sovereign nations are well-advised to acquire and cultivate intelligence from their own sources and their own data collection and analysis processes. This presupposes a lot of know-how and resources. Arguably, the more one invests in this capacity, the more attractive one becomes as an intelligence partner for foreign services. This may in turn ensure a constant and increasingly automated exchange of (relevant) data.

A key instrument for the generation of intelligence remains the interception, collection, management, and transfer of enormous troves of data that is transmitted via different telecommunications networks (fixed telephone lines, mobile networks, the internet, and satellite networks). To make it more concrete, the BND can reportedly copy 1.2 trillion IP connections per day at the world's largest Internet Exchange Point DE-Cix alone. The

foreign connections are intercepted as electronic signals, comprising various types of metadata as well as content. The acquisition process, the data minimization (i.e. the use of various filters so as to collect only that which is relevant and lawful) and the subsequent data processing and analysis require substantial human and technical resources. Moreover, given that this is financed by tax money, it is also important to ensure that the money is spent appropriately and that there is sufficient return on investment.

> **To ensure public trust in the process of democratic control, oversight bodies need to report regularly on their review work, their decision-making and the suitability of the accountability mechanisms they use.**

Clearly, though, it is not just those in the Chancellery and in the BND leadership who have vested interests in how Germany uses this formidable digital power. Next in line, but by no means in full alignment, are the internet service providers. They can be compelled to provide the government with access to their infrastructures. Just like the hundreds of government analysts and officials involved in the signals intelligence (SIGINT) process, they are keen to have the certainty that their conduct is lawful. In addition, there are other branches of government and civil society at large who share interests that go beyond the efficacy and legality of German SIGINT measures. The use of these powers needs to be legitimate and in keeping with Germany's broader human rights obligations under domestic and international law. A comprehensive and codified legal base for the use and oversight of these powers is therefore in order. This necessitates the involvement of parliament, which needs to pass a proper law. In other words, the executive branch cannot operate solely on the basis of executive decrees when it comes to such an important but also potentially rights-infringing capacity. Further, there have to be adequate safeguards and purpose limitations written into the law to protect both citizens and foreigners against undue surveillance and abuse. To ascertain whether or not these safeguards are sufficient and adhered to in actual practice requires the direct involvement of judicial and parliamentary oversight bodies. In order to ensure public trust in the process of democratic control, oversight bodies need to report regularly on their review work, their decision-making and the suitability of the accountability mechanisms they use. Depending on their mandate, they must also notify persons who have been subjected to surveillance. For those affected, the state then also has to offer judicial redress proceedings. This list is by no means exhaustive but sufficient, I hope, to show that in liberal democracies, the legality and legitimacy of signals intelligence needs to be independently assessed and not just proclaimed by those using this formidable digital power.

Returning to the zero-sum claim mentioned earlier, whatever is done in the interest of legitimacy and good democratic practice needs to be aligned with additional legitimate government interests. For example, the democratic control of SIGINT should not interfere with the government's need and responsibility to reach a decision, sometimes swiftly. More specifically, the German Constitutional Court grants the federal government a core area of sole executive responsibility (Kernbereich exekutiver Eigenverantwortung), which is generally off-limits for inquiry committees of the Bundestag. Thus, when it comes to executive deliberation on ongoing operations, the government is entitled to have a space for its own decision-making. However, this does not apply to judicial oversight, where the government often needs ex ante authorization for surveillance measures. It also cannot preclude parliamentary

review of decisions and deliberations concerning inactive operations. Furthermore, governments need to ensure that information originating from international partner agencies is handled with the necessary diligence in data security: It must not leak or become vulnerable to exploitation by a wide range of third parties.

> **Admittedly, it is a very complex undertaking to find an appropriate level of SIGINT governance that manages to honor all these seemingly conflicting interests and obligations.**

Admittedly, it is a very complex undertaking to find an appropriate level of SIGINT governance that manages to honor all these seemingly conflicting interests and obligations. It is a constant work in progress and there is no blueprint for maintaining a balance. Each democratic system operates according to different constraining and enabling factors. The next section will illuminate the dominant factors that determined Germany's unique trajectory. This much should already be clear from the outset: A general "security trumps freedom" approach is off balance and perpetuates a false conception that oversight is a security hazard: One step in the direction of freedoms is not necessarily tantamount to a step backwards, in the direction away from security.

In addition, not all interests are legitimate. Ridding the system of illegitimate interests might be an illusory goal, but it surely helps to be mindful of them when defining one's course of action. For example, one can point to the tendency in government circles to over-classify and thereby protect Herrschaftswissen (restricted knowledge that gives power over others). With hindsight, some government officials have admitted that quite a lot of classified material could have been in the public domain or at the very least shared with vetted oversight professionals. Clearly, executive bodies tend to harbor reservations regarding effective oversight, as it sheds light on their performance and may generally mean further scrutiny, work, and public exposure for them or their secrets. At the same time, the incentives of overseers can also be questionable, particularly in parliament. The media, too, can fail in playing its scrutinizing role, becoming distracted with ad hoc situations and scandals, which tend to get far more attention than the less glamorous but far more important regular business of objective oversight and balanced reporting. The result can be detrimental politicization of intelligence. However, sometimes a degree of politicization can be a good thing in a democracy: It may encourage necessary reforms and can be seen as part of the normalization of an important policy field that has been in the shadows for too long.

2. Germany's Unique Legal Trajectory on Foreign Intelligence Collection

The Snowden revelations attracted attention not just to the practices of the FIVE EYES intelligence alliance (United States, United Kingdom, Australia, Canada and New Zealand) but also to the national SIGINT practices and their legal frameworks in many European countries. Over the course of the past seven years, several nations have witnessed inquiries, reforms, and referendums as well as new jurisprudence in both European and national courts as a result of litigation by a wide range of actors. Some of the reforms of intelligence legislation may have been triggered because of genuine concerns for democratic principles and human rights, but many parliaments used these reforms as an opportunity to address new possibilities brought about by the rapid evolution

of technology and to write new powers into the law so as to create legal certainty for the operators.

These challenges to the democratic governance of SIGINT may be common to many countries, but Germany's experience has been particularly turbulent and merits further attention. The next section therefore seeks to identify the relevant explanatory factors for the reform process. It also addresses how this unique trajectory might now contribute to the international quest for adequate safeguards and effective oversight mechanisms unleashed by key judgements of the European Court of Justice and the European Court of Human Rights.

2.1. How an Extra-legal Power Could Grow in the Shadows Until 2016

When former judge and member of an influential oversight body Bertold Huber published an article in 2013 convincingly arguing that a substantial part of German foreign intelligence lacked a sufficient legal basis and as such may be incompatible with Germany's Basic Law, the effect was earthshattering for the intelligence community. Among other things, it became one of the triggers for the installment of an ad hoc inquiry committee in the Bundestag on NSA-BND cooperation, which provided many opportunities for the public to learn many more details about the BND's massive collection of foreign-foreign data than previously known. The BND referred to the collection of foreign-foreign data as "routine surveillance," and experts estimated that it amounted to ninety percent of all BND SIGINT activities in 2015.

The very authority of the BND in the field of strategic surveillance of foreign telecommunication data failed to be addressed in German intelligence legislation.

The founders of Germany's Basic Law considered intrusions into the constitutionally protected privacy of communication so severe that the law was worded to mandate them only within strict limitations. Article 10 of the law (which establishes the right to privacy of communication) clearly defines cases in which derogations are possible and sets parameters for the scope, purpose limitations, and the authorization and oversight processes necessary to enable the three federal intelligence services to lawfully engage in communication surveillance.

Yet, the very authority of the BND in the field of strategic surveillance of foreign telecommunication data failed to be addressed in German intelligence legislation up until December 2016, when the first limitations were introduced (more on this, in the next section). Prior to that time, when pressed, the government pointed to a vague general provision on the mandate of the foreign intelligence services in the BND Act as sufficient legal basis. Moreover, there had been no sufficient legal basis for independent oversight. Stated otherwise, prior to the implementation of the first BND reform, the vast spectrum of executive conduct in the realm of SIGINT bypassed not just the general public but also the supervisory bodies of the Bundestag. The government's legal interpretations justifying strategic surveillance of foreign telecommunication were not independently assessed. The same was true for the handling of collected data and their transfer to third parties. Neither the parliamentary intelligence oversight body (Parlamentarisches Kontrollgremium, PKGr), the G 10-Commission nor the Data Protection Commissioner (Bundesbeauftragte für Datenschutz

und die Informationsfreiheit, BfDI) had any say on the matter. As a result, the executive branch infringed the fundamental right to privacy of millions of people without any mitigation in the form of safeguards and oversight guarantees.

This revelation, emerging from Huber's 2013 article, outraged the opposition in parliament and various persistent and well-organized civil society actors and media professionals, some of which turned their anger into constructive reform proposals. Ultimately, mostly due to pressure for more legal certainty from within, the government coalition in the Bundestag adopted the first legal framework in Germany's history for this important practice, which included some purpose limitations and oversight requirements.

2.2. First Attempt: An Unconstitutional Retrofit

The so-called BND Reform 1.0 came into effect in December 2016. It placed much of the BND's foreign communications data surveillance on legal footing. Much of what had been absent before was now addressed in the complex technical provisions of the new law. However, the reform did not remedy the country's woefully inadequate judicial oversight system. Unlike the United States or Sweden, to name just two prominent examples, Germany did not establish a court-like institution for the judicial authorization of surveillance powers. Instead, paradoxically, the 2016 reform paved the way for further retreat of judicial oversight in Germany. It emphasized parliamentary oversight at the expense of proper powers of judicial review. This is an important difference, as only the latter possesses the authority necessary to order the cessation of ongoing surveillance measures. By and large, the BND Reform 1.0 was an inadequate response to the astounding breadth of intelligence governance deficits left unaddressed. While the reform introduced a few important steps in the right direction, it contributed to the fragmentation of German intelligence oversight institutions. Taken together, these factors rendered them far too weak in terms of access, tools, and resources to actually rein in the BND.

The executive branch infringed the fundamental right to privacy of millions of people without any mitigation in the form of safeguards and oversight guarantees.

The BND Reform 1.0 did, however, lead to some meaningful changes. In addition to providing a basis on which future reforms could build, it created an explicit ban on the use of foreign-foreign communication surveillance for the purpose of economic espionage. It also instituted important improvements in the legal basis for SIGINT cooperation between the BND and its foreign intelligence partners. More specifically, it determined that any new cooperation between the BND and foreign intelligence partners required a prior written administrative agreement on the aims, nature, and duration of the cooperation. Moreover, the executive had to inform the parliamentary intelligence oversight body about all such agreements. Another important novelty addressed joint databases with foreign intelligence services and conditions the BND had to adhere to prior to supplying them with data. The law demanded, for example, that the BND keep detailed documentation of the information it shares with foreign intelligence partners. As an added protection, the German Federal Data Protection Authority (BfDI) had to be consulted and it could review the creation of new databases by the BND as well as the data that the BND

contributed to joint databases. The reform also established new direct ministerial responsibility for SIGINT collection orders.

However, the reform failed to address one key caveat: It did not extend the restrictions that bind the German state authority in its domestic conduct also extraterritorially, i.e. for conduct beyond German borders and directed at foreigners abroad. Stated otherwise, under the BND Reform 1.0, the infringements of the privacy rights of millions of data holders all over the world by the German practice of bulk collection continued to be regarded by the German government as outside of the scope of the national legal framework. To justify this, the government invented questionable legal theories that few renowned legal scholars found convincing. One key explanation for the government's stubbornness has to do with the fact that any genuine concession would have meant a complete overhaul of the administrative procedures and oversight regime. Granting rights to foreigners under Article 10 and Article 5 of the German Basic Law would have meant a tremendous further investment in judicial oversight. That was not in the government's interest.

Had the German government accepted the premise of extra-territorial protections when BND Reform 1.0 passed into legislation, it would have tied nicely to Germany's diplomatic efforts in the United Nations in the wake of the Snowden disclosures, where Germany, together with Brazil, circulated a draft resolution that urged all member states to do more for the protection of privacy in the digital age. More precisely, UN Resolution 68/167 called upon all states 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, with a view to upholding the right to privacy."

The reform failed to address one key caveat: It did not extend the restrictions that bind the German state authority in its domestic conduct also extraterritorially.

In essence, though, Germany only woke up to the need to protect the privacy of foreigners from its own foreign intelligence collection in May 2020, when the German Constitutional Court ruling on the BND Reform 1.0 found it to be largely unconstitutional. The decision was prompted by a constitutional complaint filed in December 2017 by an alliance of the Gesellschaft für Freiheitsrechte ("Society for Freedom Rights," in German, or GFF) and five media organizations. Among other things, the case raised the fundamental question of whether German authorities abroad are at all bound by the basic rights stipulated in the German constitution. Interestingly, the Constitutional Court held a rare oral hearing in January 2020 to prepare its judgement on the case. It focused to a large extend on the deficits of German intelligence oversight, for example its fragmentation, its limited access and review powers, and its insufficient judicial oversight structures. In its May 2020 decision, the Federal Constitutional Court delivered a well-reasoned and balanced judgement which unequivocally affirmed that, when conducting bulk collection against non-nationals outside of Germany, the BND must respect their fundamental right to privacy of telecommunications and the freedom of the press. Thus, the BND Act, as amended in 2016, needs to be substantially rewritten. This concerns both the mandate and the accompanying procedures for the authorization, administration and oversight of strategic foreign-foreign telecommunication surveillance, including the provisions for automated data transfers and international SIGINT cooperation.

2.3. Current Reform Plans

As a result of the insufficient safeguards and oversight frameworks written into the BND Reform 1.0, the law must now be substantially rewritten by the end of 2021. While the Court essentially cemented bulk collection as a very potent instrument in the toolkit of the German foreign intelligence service, it also called on the Bundestag to write a whole range of safeguards into the law, so as to ensure that it will be practiced lawfully and in keeping with the Constitution and with Germany's international human rights obligations. In its ruling, the Court enumerated the necessary changes, consistent with what cyberlaw expert Graham Smith calls "end-to-end oversight."

Germany must now create proper judicial oversight bodies with ample access, tools, and resources to authorize the surveillance orders in this field and to ensure that the various steps of data processing and transfers comply with the long list of safeguards it demanded. The Court ruling conceived this in the form of what are essentially two structures for judicial oversight in Germany: "On the one hand, it must be ensured that the key procedural steps of strategic surveillance – partially also ex ante – are subject to an oversight regime that resembles judicial review and entails the power to make final decisions. On the other hand, the measures must be subject to an administrative oversight regime that can conduct randomized oversight of the legality of the entire surveillance process on its own initiative." Importantly, at least for the de facto potency of oversight, the Court also demanded that "the effectiveness of both the controls in practice and the legal regulations must be evaluated at regular intervals" and specified that the "material resources must have a scope that allows, for example, effective control of the filter processes for separating the communications of Germans from those of non-nationals and for the protection of confidential relations and, if necessary, to develop separate files and control programs for this purpose."

> **Given the rapid advances in surveillance technology, it is high time to explore how automation and artificial intelligence might also be beneficial to the democratic control of security agencies.**

Notice how the latter points to an important new frontier for intelligence oversight: new supervisory technology to keep pace with high-tech intelligence. Indeed, a whole reform agenda for modern, data-driven intelligence oversight is waiting to be addressed once review bodies in Germany receive sufficient access to the operational systems and databases of the government. Given the rapid advances in surveillance technology, it is high time to explore how automation and artificial intelligence might also be beneficial to the democratic control of security agencies. Recent research has suggested ways in which supervisory technology might be used to engage in pattern matching and other scrutiny tasks to alert overseers about potential data misuse, possibly by means of push notifications.

> **It is not enough to tighten standards and oversight in place in a given country when its international partners operate under no comparable constraints.**

A further important clarification emerged of a decision by the Federal Constitutional Court in Karlsruhe: Given the magnitude of international intelligence cooperation, future judicial oversight bodies must be exempt from the so-called "Third

Party Rule." Thus, future intelligence sharing arrangements will have to include provisions whereby the originator of shared information will accept that the German judicial oversight bodies will be given access to shared material so as to effectively review Germany's lawful conduct.

There is not enough room here to expand on the long list of safeguards that should now be included in the BND Reform 2.0, but in what follows, I will highlight a few more that might help to set new international standards regarding rights-based surveillance. Consider, for example, the requirement that if foreign-foreign strategic surveillance is collected for the sole purpose of assisting in decision-making of the Federal Government, then such data should be generally regarded as "hands-off!" when it comes to international data transfers. The Court also demanded special safeguards to provide greater protection for persons whose communications demand client confidentiality – not just in Germany but also abroad.

3. An Opportunity for the Harmonization of Common Standards and Safeguards

New safeguards and better purpose limitations in national intelligence legislation are decisive in protecting rights holders against disproportionate government access to their data. However, especially in light of intense international intelligence cooperation and increased levels of surveillance generally, it is not enough to tighten standards and oversight in place in a given country when its international partners operate under no comparable constraints. This is, unfortunately, still very common and as long as it remains so, there is a great risk of creative non-compliance and accountability evasion by means of international cooperation. This, in turn, can jeopardize the gains made by domestic reforms.

Luckily, there are new grounds for optimism. The practice of bulk collection and its democratic control has won the renewed attention of journalists, lawmakers, and oversight bodies due to key judgements by the European Court of Human Rights and the European Court of Justice (CJEU) in 2020. In addition, the Council of Europe issued an important statement urging member states to enable more effective oversight of intelligence services and to ratify Convention 108+, the only international agreement that deals with data processing and safeguards in the area of national security.

More specifically, in another groundbreaking ruling known as Schrems II, the CJEU argued that neither the scale of US intelligence activities nor the level of protection and possibility for effective and enforceable individual redress conform to an equivalent standard set out by the General Data Protection Regulation (GDPR). The CJEU found that appropriate safeguards against disproportionate government access to data as well as enforceable rights and effective legal remedies are crucial and should be extended to non-nationals. In essence, this is similar to what the German constitutional court underlined in its May 2020 judgement: When conducting bulk surveillance, foreign intelligence services and their respective legal frameworks should respect the fundamental right to privacy of foreign nationals abroad. Judicial oversight institutions and procedures ought to be adjusted to ensure this happens in practice.

Finally, the October 6 CJEU judgements underscored that "national security concerns do not exclude EU Member States from the need to comply with general principles of EU law such as proportionality and respect for fundamental rights to privacy, data protection and freedom of

expression." Thus, I now see a new opportunity for promoting common standards to protect against disproportionate government access to communications data and to promote the professionalization of oversight. Interestingly, it is not only policy experts in government, parliament and civil society who will keep an eye on oversight surveillance legislation and its safeguards. Tech companies, as well, will have an interest as they try to avoid adhering to different rules when transferring data.

Looking at the intelligence reforms that will occupy the Bundestag this fall and winter, it is likely that Germany might contribute to good standards, for example when it comes to safeguards concerning data transfer to international security agencies. Another potential avenue for better practices might be the implementation and professionalization of proper end-to-end oversight, the inclusion of non-nationals as right holders in domestic intelligence legislation, and new safeguards regarding the data of protected groups such as journalists, priests or doctors.

4. Conclusion

Western democracies once allowed mass surveillance to grow unchecked in their shadows. Following the revelations of Edward Snowden in 2013, some democracies introduced significant reforms. Many of those reforms, arguably, were designed first and foremost with the objective of securing the continuation of a sweeping practice and to establish legal protections for those involved in the process. The fact that Germany now faces the opportunity to create a true and much needed intelligence reform can largely be credited to the tenacity of a group of civil society organizations, who won their strategic litigation against the government in front of an independent court that took the matter very seriously.

The fact that Germany now faces the opportunity to create a true and much needed intelligence reform can largely be credited to the tenacity of a group of civil society organizations.

While it is very encouraging that the Bundestag is now being given a second chance to pass a more comprehensive and constitutional intelligence legislation, the proof will be in the pudding. As the text has suggested, there are various different interests at play, and even if German lawmakers manage to successfully address the long list of safeguards that the Constitutional Court demanded, a lot of work lies ahead for closing accountability gaps in the realm of intelligence cooperation. Luckily, though, the recent jurisprudence of the European Court of Justice and the European Court of Human Rights unleashed a new search for better standards and effective oversight to protect right-holders against disproportionate government access to data. It is indeed time to push for a European acquis on non-targeted surveillance, for the topic to be addressed in European Union law – and this will take a lot of political will, not just in Berlin.

Endnotes

[1] UK Government. (2016). The operational case for bulk powers. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

[2] Anderson, David. (2016). Report of the bulk powers review. Available at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf. p. 120.

[3] Anderson (2016), p. 4.

[4] Naturally, there are also other intelligence powers that merit further attention. This would, however, go beyond the scope of this paper. Briefly, though, four methods to acquire bulk data have increasingly been written into modern intelligence legislation. Next to the "bulk interception of communications", there is "bulk equipment interference", "bulk communications data obtained from communications service providers", and the acquisition of "bulk personal datasets" (UK Government 2016). The German Bundestag has yet to place "bulk equipment interference" (aka bulk hacking), i.e. "the acquisition of communications and equipment data directly from computer equipment overseas" (Ibid) on a solid legal footing. The foreign intelligence draft legislation which became known to the public in September 2020 now introduces a separate legal basis for computer network exploitation.

[5] This includes, but is not limited to, (bulk) hacking, effects operations on social media accounts or the acquisition of large datasets from the private sector.

[6] As regards different intelligence operations by the German armed forces, further details can be found in: Siemsen, Annelie. (2018). Der Schutz personenbezogener Daten bei der Auslandsaufklärung durch Bundeswehrsoldaten. Berlin: Duncker & Humblot; and Schulze, Matthias. (2020). German Military Cyber Operations are in a Legal Gray Zone. Available at: https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone.

[7] Hoppenstedt, Max, and Wiedmann-Schmidt, Wolf. (2020). So überwacht der BND das Internet. Available at: https://www.spiegel.de/netzwelt/netzpolitik/bundesnachrichtendienst-so-ueberwacht-der-bnd-das-internet-a-216ebe9a-6f22-4883-b1c9-ac5d1442497a.

[8] The annual budget for the three federal German intelligence services amounted to roughly 1.4 billion Euros in 2019.

[9] Albeit with different degrees of intensity, this holds true for France, the Netherlands, Sweden, Norway, Switzerland, Belgium and Germany, to name just a few countries.

[10] Rath, Christian. (2003). Auslandsüberwachung des BND: Grundgesetz gilt auch im Ausland. Available at: https://taz.de/Auslandsueberwachung-des-BND/!5060992/.

[11] Löffelmann, Markus. (2015). Regelung der "Routineaufklärung". Recht und Politik 6, p. 2. Available at: http://www.recht-politik.de/wpcontent/uploads/2015/06/Ausgabe-vom-22.-Juni-2015-Regelung-derRoutineaufkl%C3%A4rung-PDF-Download.pdfhttp://www.recht-politik.de/regelung-der-Routineaufklarung/.

[12] Wetzling, Thorsten (2017). Germany's intelligence reform: More surveillance, modest restraints and inefficient controls. Available at: https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

[13] United Nations. (2014). Resolution 68/167: The right to privacy in the digital age. Available at: http://undocs.org/A/RES/68/167.

[14] Wetzling, Thorsten. (2020). Try harder, Bundestag! Germany has to rewrite its foreign intelligence reform. Available at: https://aboutintel.eu/german-constitutional-court-bnd-ruling/.

[15] Bundesverfassungsgericht. (2020). Press statement: In their current form, surveillance powers of the Federal Intelligence Service regarding foreign telecommunications violate fundamental rights of the Basic Law. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

[16] Ibid.

[17] Ibid.

[18] Vieth, Kilian, and Wetzling, Thorsten. (2019). Data-driven Intelligence Oversight. Recommendations for a System Update. Available at: https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf.

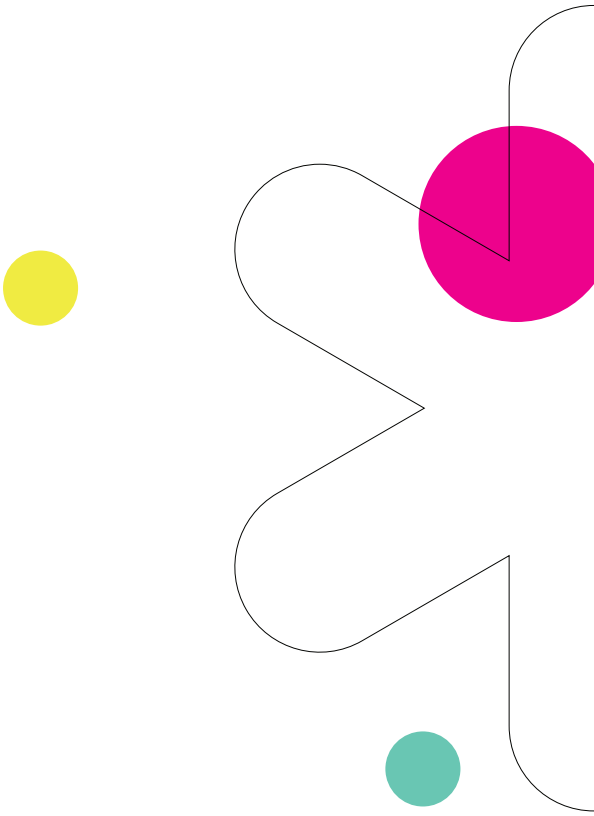
[19] Council of Europe. (2020). Joint Statement: Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services. Available at: https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb.

[20] Lomas, Natasha. (2020, October 6). Europe's top court confirms no mass surveillance without limits. TechCrunch. Available at: https://techcrunch.com/2020/10/06/europes-top-court-confirms-no-mass-surveillance-without-legal-limits/.

About the Author

Thorsten Wetzling heads the research of the Berlin-based think tank Stiftung Neue Verantwortung (SNV) on basic rights, surveillance and democracy. His work focuses on the generation of new ideas and solutions for more efficient and democratic intelligence governance in Germany and Europe. In this capacity, Thorsten directs the European Intelligence Oversight Network (EION) and is Principal Investigator in a collaborative multi-year academic research project (GUARDINT.org), designed to address and to redress the gap between increasingly transnational surveillance practices and still largely national accountability mechanisms. In 2019, Thorsten launched aboutintel.eu – a new multi-stakeholder platform for pan-European conversations on all things intelligence.

Thorsten is a member of the scientific committee of the Cyber and Data Security Lab at the Vrije Universiteit Brussel (VUB) and the advisory board on Europe/Transatlantic of the Heinrich Böll Foundation in Berlin. Thorsten holds a doctorate degree in political science from the Graduate Institute of International and Development Studies in Geneva.



Israel Public Policy Institute

Hapelech St. 7, Tel Aviv, Israel
→ office.israel@ippi.org.il
→ www.ippi.org.il

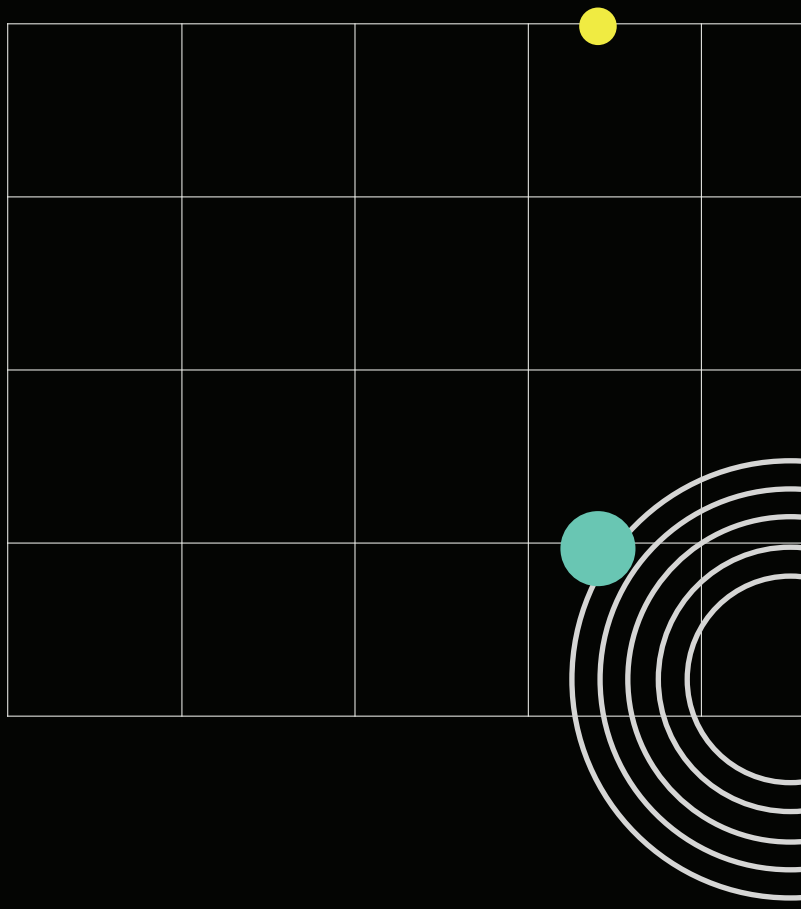
Heinrich Böll Foundation

Schumannstraße 8, Berlin Germany
→ info@boell.de
→ www.boell.de

Heinrich Böll Foundation Tel-Aviv

Har Sinai St. 1, Tel Aviv, Israel
→ info@il.boell.org
→ www.il.boell.org

Release date: November 2020



HEINRICH
BÖLL
STIFTUNG

Israel
Public Policy
Institute

HEINRICH BÖLL STIFTUNG
TEL AVIV