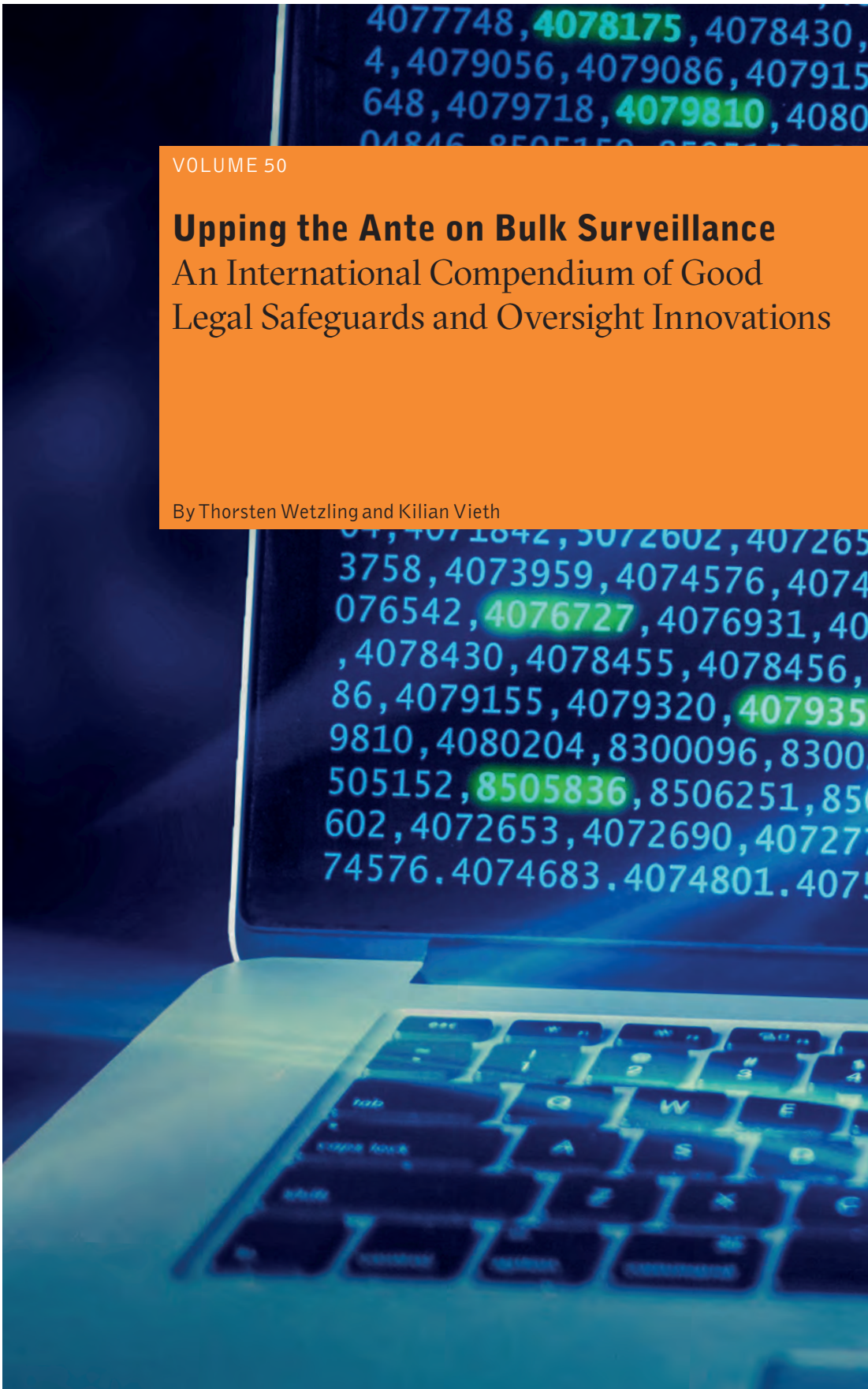
HEINRICH BÖLL STIFTUNG
DEMOCRACY



VOLUME 50

Upping the Ante on Bulk Surveillance

An International Compendium of Good Legal Safeguards and Oversight Innovations

By Thorsten Wetzling and Kilian Vieth

Stiftung Neue Verantwortung

UPPING THE ANTE ON BULK SURVEILLANCE

HEINRICH BÖLL STIFTUNG
PUBLICATION SERIES ON DEMOCRACY

VOLUME 50

Upping the Ante on Bulk Surveillance

An International Compendium of Good Legal Safeguards and Oversight Innovations

By Thorsten Wetzling and Kilian Vieth

Edited by the Heinrich Böll Foundation

The Authors

Thorsten Wetzling heads the SNV's research on surveillance and democratic governance. He directs the European Intelligence Oversight Network and is responsible for the EU Cyber Direct project's work relating to India. As an expert on intelligence and oversight, he was invited to testify before the European Parliament and the Bundestag on intelligence legislation. His work appeared in various media outlets. Recently, he became a member of the expert advisory board on Europe/Transatlantic of the Heinrich Boell Foundation in Berlin. Thorsten Wetzling holds a doctorate degree in political science from the Graduate Institute of International and Development Studies in Geneva.

Kilian Vieth manages SNV's work on government surveillance and intelligence oversight. He works on reform approaches for a more democratic and more efficient intelligence and surveillance policy in Germany and Europe. In 2018, Kilian Vieth was invited to testify before the parliament of Hesse on the regional surveillance legislation. Beyond that, his research interests include digital human rights, critical security studies, as well as political and social issues of algorithmic decision-making.

Partner Foundation

The **Stiftung Neue Verantwortung (SNV)** is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organisation adopted a concept of mixed funding sources that include foundations, public funds and businesses. Issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance now affect key areas of economic and social policy, domestic security or the protection of the fundamental rights of individuals. The experts of the SNV formulate analyses, develop policy proposals and organize conferences that address these issues and further subject areas. www.stiftung-nv.de

Upping the Ante on Bulk Surveillance
An International Compendium of Good Legal Safeguards and Oversight Innovations
By Thorsten Wetzling and Kilian Vieth
Volume 50 of the Publication Series on Democracy
Edited by the Heinrich Böll Foundation

Design: feinkost Designnetzwerk, S. Langer (predesigned by blotto design)
Cover-Photo: «Data Security» Blogtrepreneur – flickr (CC BY 2.0)
Printing: ARNOLD group, Großbeeren
ISBN 978-3-86928-187-2

This publication can be ordered from: Heinrich-Böll-Stiftung, Schumannstr. 8, 10117 Berlin
T +49 30 28534-0 **F** +49 30 28534-109 **E** buchversand@boell.de **W** www.boell.de

CONTENTS

FOREWORD

Modern democratic societies are increasingly being confronted with two difficult-to-reconcile demands of their citizens: protection against a growing number of new threats and the right to privacy. An open and vigilant democracy nevertheless can meet these requirements only in part. The difficulties have been illustrated through numerous examples involving intelligence services in recent years – ranging from the failure to prevent terrorism in the case of Anis Amri to the Edward Snowden revelations about mass surveillance by the National Security Agency.

The precarious balance between the need for security and the right to privacy will continue to characterize «risk societies» of the 21st century. The forces of globalization will furthermore push these difficult issues into new territory – be it through new threats from transnational terrorism, hybrid warfare, or novel technological monitoring capabilities such as digital face recognition. These developments call for a broad societal discussion about the appropriate risk management, which combines the effectiveness of security institutions with their democratic legitimacy.

Thorsten Wetzling, from the Stiftung Neue Verantwortung, already addressed these questions in a study for the Heinrich Böll Foundation in 2016: In our Democracy Series (Volume 43), he informed readers about the state of intelligence oversight in Germany and drew a sobering balance sheet.

With the present study, we want to broaden the discussion in two ways. We have asked the Stiftung Neue Verantwortung to look beyond the German example to the practices of intelligence oversight in a number of key countries in the transatlantic arena. At the same time, through this comparative study, we wanted to take a different approach when considering «effective oversight» and not only identify the deficits of intelligence oversight, but also highlight encouraging practices that have emerged in the respective survey countries in the wake of recently reported reforms.

Therefore, the study may well be understood as an invitation to the community of national regulatory authorities to look beyond national borders and be inspired by the best practices of their neighboring countries.

During the progressive integration of European foreign, security, and defense policies, and against the backdrop of increasing levels of cooperation between Western intelligence services, democratic oversight of these services must also be free from nation-centric views and strengthen the transatlantic exchange. This is especially true in a period of Western uncertainty and authoritarian temptations, especially within the transatlantic community. Robust oversight practices and good laws can serve as bulwarks against the erosion of fundamental rights should a government be infested with the illiberal virus that is currently rampant in Europe and America.

We hope that the present study will educate readers and fulfill both a political and social mission. At the political level, in a time of growing skepticism about the EU and NATO, we hope to promote the transatlantic dialogue on informational self-determination and, more generally, individual freedom and human rights. The study has identified encouraging examples of effective democratic intelligence oversight in many countries, examples that deserve further exploration. A liberal, value-based community relies on this exchange of «best democratic practices.»

At the societal level, we hope that questions about the suitable regulation of Western intelligence services will be given reification through this very detailed comparative study. The debate about intelligence has always suffered from a lack of professional analysis and an oversupply of empirically unverified hypotheses and conspiracy theories.

We owe it to our readers to provide them with the best possible guidance for a critical discussion on Western intelligence practices. Hopefully, they can use this study to further the debate on democratically legitimate and effective intelligence services.

Berlin, November 2018

Giorgio Franceschini
Heinrich Böll Foundation
Head of Foreign and Security Policy Division

FOREWORD

On September 13, 2018, the European Court of Human Rights ruled in the case of Big Brother Watch and Others v. the United Kingdom, examining the bulk interception of communications, intelligence-sharing, and the obtaining of communications data in light of the European Convention on Human Rights. The judgment marks the first occasion on which the Court has addressed compliance of intelligence-sharing with Article 8 of the Convention. Prior to this ruling, the Stiftung Neue Verantwortung worked hard to be able to provide you with this compendium concerning the bulk interception of foreign communications.

Addressing the complexities of bulk interception powers exercised by intelligence and security services is by no means an easy task. This is even less so where it concerns the ways in which such powers are organized and put into practice in different countries across the Western world. The Stiftung Neue Verantwortung has reached an impressive result. This compendium of good legal safeguards and oversight innovations thoroughly addresses the legal complexities of bulk interception powers. It pinpoints the need for adequate legal safeguards and the central role that oversight bodies need to play in making sure such safeguards are adhered to in practice. It provides us – the oversight bodies of both Germany and the Netherlands – with food for thought and brings us to the following mutual considerations.

Firstly, national legislation needs to provide oversight bodies with strong legal criteria to assess the use of bulk interception powers as well as with the adequate means and measures to conduct oversight. This is needed to enable oversight bodies to effectively oversee the complex processing of large volumes of data that comes with these powers. It is imperative that national legislators are aware of, and learn from, other national legal frameworks.

Next, oversight bodies need to critically reflect upon their own abilities and oversight practices in order to develop effective methods of oversight. We need to improve our technical expertise and oversight methods in order to adapt to an operational Intelligence reality characterized by technological developments and intensifying intelligence cooperation. By sharing with each other the ways in which we seek oversight innovation, we may learn from each other's efforts and best practices.

Last but not least, oversight bodies need to strengthen their cooperation in order to more effectively oversee the international exchange of data and developments toward more advanced intelligence cooperation, such as the joint processing of data and making joint intelligence products. There is an urgent need for oversight bodies to jointly search for ways to more effectively oversee such intelligence cooperation.

This compendium is an important tool for doing precisely these things. It provides us with an excellent overview of best practices in the areas of legal safeguards

and oversight developments. It gives us profound insights into the legal complexities of bulk interception and the choices that were made in structuring the national legal frameworks governing these processes. It helps us to understand the need for rigorous and effective oversight mechanisms and to identify where our own oversight practices might still fall short. Lastly, it provides us with a meaningful starting point to strengthen cooperation between oversight bodies and to find common ground in jointly overseeing intelligence cooperation.

We welcome you to carefully read through the compendium. It is an excellent read, and we invite you to take part in a still much needed international discussion.

Harm Brouwer
Chair of the Dutch Review Committee on the Intelligence and Security Services

Bertold Huber
Deputy Chair of the German G10 Commission

Abstract

Unprecedented public debates about intelligence governance following the revelations of Edward Snowden have not changed the fact that all major democracies allow their national intelligence services to intercept communications data in enormous quantities. Many people question the efficiency of bulk surveillance practices and their compatibility with fundamental rights. Others worry about its effect on the social fabric of democratic societies.

Yet, the fact is that most parliaments have expanded, rather than curtailed, surveillance powers in recent intelligence reforms. What is more, the European Court of Human Rights recently upheld the Swedish regime for bulk interception of foreign communications and called the practice a «valuable means» of counterterrorism in its Big Brother Watch decision of September 2018. Therefore, one can assume that the practice of bulk communications surveillance is here to stay. If that is the case, then it is high time to subject national legal frameworks and their corresponding oversight systems to a comparative review and to identify good practices. National courts and the European Court of Human Rights, alike, have frequently admonished national governments for flaws or shortcomings in the oversight regime. In the September 2018 decision, the European Court of Human Rights again demanded more rigorous and effective oversight mechanisms.

Yet, especially as surveillance technology is rapidly evolving, what exactly constitutes effective oversight of bulk collection in actual practice? A court will not design new rules or prescribe specific accountability mechanisms. This is the difficult and necessary work of democratic governance, and it needs to be done by the principled members of the different oversight bodies that understand the critical importance of their work.

This study presents individual examples of legal provisions and oversight practices that, by comparison, stand out as more balanced or more innovative responses to the many thorny challenges that ought to be met. The resulting compendium features a wide range of high-water marks from different national surveillance regimes. It shows that each nation – despite constitutional and political differences, and irrespective of individual reform trajectories – has a lot to learn from its international partners. These practices, we believe, should be widely promoted, for they increase the legitimacy and effectiveness of a controversial practice that is here to stay.

I. Introduction

All democracies rely on intelligence agencies to keep their open societies safe. They provide actionable intelligence to decision-makers on a wide range of security and foreign policy matters. Regardless of whether this concerns terrorism, arms proliferation, or organized crime,[1] this requires information beyond that which is publicly available. Intelligence services master a range of clandestine methods to acquire such information. Some methods – including the electronic surveillance of communications data – are difficult to reconcile with the fundamental principles of democratic governance, such as rule of law, transparency, and accountability. They may also infringe on fundamental human rights and civil liberties, such as the right to privacy as well as the rights to freedom of opinion, of expression, of association, and of assembly. In order to ensure public trust and the legitimacy of intelligence governance, democracies need to place all intelligence activities on a solid legal footing and subject them to rigorous and effective oversight.

This remains a formidable challenge.[2] Admittedly, the democratization of intelligence and the professionalization of oversight has made significant advances over the last few decades in many established democracies. Parliaments in Europe, North America, and Australasia, for example, frequently reformed national intelligence laws and extended the remit and the resources of independent oversight bodies over time. In addition, countries such as the United States have introduced transparency principles that commit the intelligence community to provide more information to the public than at any previous time in history.[3] Still, as the failures of effective oversight of electronic surveillance prior to the revelations of Snowden have shown, democratic intelligence governance cannot be taken for granted. The stakes are high, and the temptations to abuse privileges such as government secrecy are omnipresent. The

1 Naturally, these are just a few common security threats that concern intelligence services the world over. Which particular threat or national interest a particular service is tasked to look into varies from service to service.

2 Recent experiences and future challenges of democratic control of intelligence in different contexts are discussed, e.g., in Goldman and Rascoff (eds.),«Global Intelligence Oversight. Governing Security in the Twenty-First Century,» 2016; Leigh and Wegge (eds.), «Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World,» 2018; Anderson, «New Approaches to Intelligence Oversight in the U.K.,» January 2, 2018, https://www.lawfareblog.com/new-approaches-intelligence-oversight-uk; Wetzling, «Options for More Effective Intelligence Oversight,» 2017, https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

3 U.S. Principles of Intelligence Transparency for the Intelligence Community, accessible via https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

legitimacy of intelligence action must constantly be earned – even in the presence of severe security threats. Effective governance and democratic control of intelligence is the result of a complex, multi-facetted effort that cannot be left to a small group of technocrats. Next to audits within the services, it requires rigorous executive control and parliamentary oversight. It also needs strong, independent, and tech-savvy judicial mechanisms to either authorize or approve and review individual intelligence measures. In addition, there ought to be independent public scrutiny over the process of intelligence legislation and the oversight practices. Together, these various layers of oversight and accountability mechanisms provide input legitimacy to intelligence governance. What is more, they also ensure that the output of intelligence policies and decisions are informed and effective (output legitimacy).

Intelligence governance is also very much a work in progress rather than a finished product. There ought to be regular updates to intelligence legislation and the oversight frameworks due to the pace of technological change. It brings new tools or entirely new practices to the field, some of which oversight bodies should also use in order not to lag behind and to become more efficient.[4] Similarly, political pressure for stronger collective security or new revelations of intelligence malfeasance can prompt new reviews of the governance framework. What is more, and not just in the United Kingdom, it appears that «many of the daily activities of the security agencies are left unregulated by law. Key issues of targeting, processing, and liaison with other agencies at home and abroad are doubtless the subject of internal governance but little is disclosed to the public and even less is set in legal format.»[5]

Put simply, when democracies allow their intelligence services to deploy digital surveillance powers in the name of national security, they have to do this within the rubric of the rule of law and checks and balances. And while cultural, political, and constitutional differences among those nations render it futile to establish a one-size-fits-all intelligence governance blueprint, it is certainly worthwhile to study how common challenges are met across different systems and to identify and promote innovative solutions so that they may traverse national jurisdictions.

In this compendium, we focus on the bulk surveillance of foreign communications. By this, we mean the interception, collection, management, and transfer of enormous troves of communications data that is transmitted via different telecommunications

4 For a recent account of how artificial intelligence (AI) methods are used for the analysis of large datasets, see, e.g., Hoadley and Lucas, «Artificial Intelligence and National Security,» April 26, 2018, 9, https://fas.org/sgp/crs/natsec/R45178.pdf.

5 McKay and Walker, «Legal Regulation of Intelligence Services in the United Kingdom,» 2017, 1887. For a recent overview of unanswered questions when it comes to international intelligence sharing, see: International Network of Civil Liberties Organizations, «Unanswered Questions – International Intelligence Sharing,» June 2018, https://www.inclo.net/pdf/iisp/unanswered_questions.pdf. In Germany, for example, the acquisition and subsequent use of data that may have been collected by private companies or the military, and which may be used and modified by the intelligence services, remains to be placed on a more solid legal footing. See: Wetzling, «Germany's intelligence reform: More surveillance, modest restraints and inefficient controls,» 2017, 13–16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

networks (fixed telephone lines, mobile networks, the internet, and satellite networks). The foreign communications are intercepted as electronic signals, comprising various types of metadata as well as content. It is controversial because it is «non-targeted» or «unselected» or «general» – in other words, not directed at a particular individual.[6] David Anderson, the former UK Reviewer of Terrorism Legislation, warned that the use of bulk powers may have serious adverse human rights implications: such powers «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 […] any abuse of those powers could thus have particularly wide ranging effects on the innocent […] even the perception that abuse is possible, and that it could go undetected, can generate corrosive mistrust.»[7]

Bulk surveillance of (foreign)[8] communication has been a standard intelligence practice for decades. Greater public interest in the wake of the Snowden revelations, and the fact that many countries lacked a robust legal framework for it, let alone effective oversight thereon, has led many parliaments to adopt new laws or to amend existing legislation since then. Now that a sweep of new laws, oversight institutions, and control practices are in place, and now that the European Court of Human Rights has decided – in July 2018 and in September 2018 – that the practice of bulk surveillance of foreign communications can be compatible with the European Convention on Human

6 Many countries, including Germany and the United States, apply different legal frameworks for the bulk surveillance of foreign traffic. Communications that have both their origin and destination outside the intercepting country are treated differently than communications where one end involves the territory of the intercepting agency. Others, such as the Netherlands, do not distinguish between foreign and domestic communication when it comes to bulk surveillance. Whether or not surveillance legislation can legally discriminate against non-nationals, and whether or not it is technologically possible to enforce different data protection regimes, is a matter of much contention. See, e.g., Swire, Woo, and Desai, «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft),» 2018, or Lubin, «We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,» 2017, https://papers.ssrn.com/abstract=3008428. Yet, there are also strong arguments against this practice, see, e.g., the recent challenge against the new German intelligence law or the expert testimony that elaborates on the technical shortcomings of the current data minimization practice in Germany: Rechthien, «Sachverständigen-Gutachten gemäß Beweisbeschluss, 1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestages,» September 2016, https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf.

7 Anderson, «Report of the Bulk Powers Review,» 2016, 9.6., https://nls.ldls.org.uk/welcome.html?ark:/81055/vdc_100035016622.0x000001.

8 Some countries have detailed laws that regulate the bulk collection of domestic-foreign communications, but they may not have an explicit legal regime for foreign-foreign communications. Others do not distinguish between foreign and domestic communications at all in their respective intelligence legislation. Although we try to address the governance of bulk communications surveillance in general, at some points the specific reference to foreign communications becomes important for the application of legal safeguards and oversight practice. In such a case, a specific reference to the provision is made.

Rights,[9] itis a good time to take the national governance regimes at face value. While pending litigation at both national and European courts may still prompt a re-design of some intelligence laws, the very practice of bulk surveillance of communication is unlikely to be abandoned. Quite the contrary, it is here to stay and will remain a key practice of modern intelligence.[10]

This makes it all the more important, then, to identify good solutions to the many thorny governance challenges that it entails. This is what we aim to provide with this publication. More specifically, the compendium identifies and contextualizes legal provisions and current oversight practices from different democracies on bulk foreign communications surveillance that – by comparison – stand out for either their compatibility with democratic governance, the rule of law, or the protection of human rights. They are also seen as good practices when they embody an innovative attempt to improve the effectiveness of oversight.

We believe that all countries stand to benefit from a thorough discussion on the growing acquis of good practices regarding the governance and oversight of bulk surveillance of (foreign) communications. Despite the relevant and legitimate criticisms that can be directed at recent intelligence reforms,[11] most of them also brought about individual changes that embody significant improvements in governance. When taken together, these promising practices paint a unique picture, which, in turn, can help identify opportunities for progress in national frameworks. Obviously, it takes knowledge to develop a reform agenda and political will to overcome national shortcomings. Yet, if other countries successfully demonstrate that the sky did not fall when they implemented more ambitious solutions to particular governance challenges, then this can be used as a powerful argument to persuade others to follow suit.

9 European Court of Human Rights, «Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08),» 2018, http://www.statewatch.org/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf.

10 The advancement of encrypted communication does, however, put additional weight on techniques such as computer network exploitation and the exploitation of software vulnerabilities.

11 Lubin, «Legitimizing Foreign Mass Surveillance in the European Court of Human Rights,» August 2, 2018, https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

II. Methods

When democracies allow their intelligence services to conduct large-scale electronic surveillance of foreign communications data, they must do so within the limits of the law. They must also ensure that this practice is subject to effective and independent oversight. Yet, what does that mean in practice, and how can one best distinguish between good and poor legal safeguards and efficient and inefficient oversight dynamics?

To find out, we studied a wide range of different public resources, such as commentary on intelligence laws, oversight body reports, strategic litigation materials, as well as commentary on intelligence policy.[12] We developed our own analysis scheme (see below) and conducted a series of interviews with a range of different experts (legal scholars, computer scientists, public servants and oversight professionals, industry representatives, etc.) to obtain further information on current practices. Once we had

12 For some recent accounts of new intelligence legislation and the reform of oversight mechanisms concerning Canada, France, Germany, the United Kingdom, the United States, as well as some comparative reviews, see: Forcese, «Bill C-59 and the Judicialization of Intelligence Collection. Draft Working Paper 04-06-18,» 2018; Parsons, Gill, Israel, Robinson, Deibert, «Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters), First Reading (December 18, 2017).» The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2017, https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf; Chopin, «Intelligence Reform and the Transformation of the State: The End of a French Exception,» 2017, https://doi.org/10.1080/01402390.2017.1326100; Ohm, «The Argument against Technology-Neutral Surveillance Laws,» 2010, https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=; Tréguer, «From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France,» October 2016; Schaller, «Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden,» 2018; Wetzling,«Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficent Controls,» 2017, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf; Anderson, «A Question of Trust: Report of the Investigatory Powers Review,» 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf; McKay, Blackstone's Guide to the Investigatory Powers Act 2016, 2018; Smith, «A Trim for Bulk Powers?,» September 7, 2016, https://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html; Donohue, «The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law,» 2017, https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law; Wizner, «What Changed after Snowden? A U.S. Perspective,» 2017; European Union Agency for Fundamental Rights, «Surveillance by Intelligence Services – Volume I: Member States› Legal Frameworks,» October 22, 2015, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services; European Union Agency for Fundamental Rights, «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update,» 2017, http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega.

collected enough information, we wrote a draft compendium and organized two expert workshops – one with oversight body representatives in May 2018, and one with European and North American civil society experts in June 2018 – to further test and refine our findings.[13]

Based on this work, we can now present this compendium of *good practices on bulk surveillance of (foreign) communications* from different national intelligence laws and oversight systems across Europe, North America, and Australasia. The compendium is by no means meant to be exhaustive, and we invite your comments and additional suggestions. If a particular example is taken from one country, this does not exclude the possibility that the same, or similar, rule or practice exists in another jurisdiction.

We consider a practice to be good when, by comparison, it provides an improved safeguard against potential violations of rights, or because it stands out in the way that it solves a common governance challenge, or because it may make innovative use of technology for the benefit of greater oversight effectiveness.

Although our method may allow us to identify international high-water marks regarding the governance and control of bulk surveillance of communication, we do not hold enough information to rate the overall quality of individual surveillance laws or national oversight frameworks. Too many individual factors contribute to this, and we cannot reflect on all of them here.[14] Moreover, there are limits to what a comparative study of this kind may reveal. Every country has its unique social, legal, and political setup that influences the governance and reform of intelligence. As we do not account for these differences here, we cannot credibly make declarations on the overall governance framework in which these good practices are embedded. This also means that the amount of citations that a national law or oversight regime receives in this compendium cannot be construed as a suitable indicator for the overall quality of the bulk surveillance regime in each country.

Our focal points are the legal frameworks and oversight regimes regarding non-targeted signals intelligence (SIGINT), with a special emphasis on foreign communications data.[15] This provides intelligence services «mass access [...] to data from a population not itself suspected of threat-related activity.»[16] Unsurprisingly, then, non-targeted (or «bulk») SIGINT capabilities are often considered to be the crown jewels of a national intelligence community. It is a technically sophisticated and highly complex intelligence-gathering discipline that involves a lot of international cooperation and grew in the shadows of many democracies for quite some time. The National Security Agency (NSA) of the United States famously proclaimed that, due to the shift

13 See Annex for a list of workshop participants and interviewees.

14 For an overview of those factors, see, e.g.: Richardson and Gilmour, Intelligence and Security Oversight. An Annotated Bibliography and Comparative Analysis, 2016; Zegart, «The Domestic Politics of Irrational Intelligence Oversight,» 2011; Wetzling (ed.), Same Myth, Different Celebration? Intelligence Accountability in Germany and the United Kingdom, 2010.

15 Communications data, for the purpose of this report, refers to both content of communications (e.g., the text of an email) and information about communications, also known as metadata (e.g., the email addresses of sender and recipient).

16 Forcese, 2018, 3.

toward digitized means of communication, we were now living in «the golden age of SIGINT.»[17] This said, bulk surveillance of foreign communications is but one practice in a much larger universe of intelligence-gathering disciplines.[18] Targeted surveillance and active computer network operations (i.e., getting access to datasets via hacking computer networks, etc.) are two other prominent examples. Communications data can, of course, also be collected in bulk through hacking operations.[19] Due to our own resources, and for the sake of reducing complexity, we decided to focus only on bulk collection of foreign communications here.

What are the relevant aspects that one needs to consider when it comes to creating a legal basis for – and the democratic control of – bulk surveillance? According to what standards and criteria can we assess the quality of either a legal provision or an oversight practice? Clearly, this, too, needs further unpacking. The following graph breaks down the most relevant governance aspects for bulk surveillance of foreign communications into eight phases.

Whether it is the initial strategic planning, the application processes, or the authorization/approval processes that are required prior to the execution of bulk powers, one can depict in legislation and actual oversight practices a range of relevant standards that democracies ought to meet. The same holds true, of course, for the implementation of bulk powers in practice: This, too, involves many processes and constitutional obligations that become more readily apparent when the entire cycle is depicted in its different stages. Our multi-stage model is based, in essence, on the more common intelligence cycle that has traditionally been used to explain the different stages required to produce actionable intelligence.

This compendium devotes a chapter to each of the eight phases shown in figure 1. They begin with a brief account of the typical activities in that stage before elaborating on the relevant governance aspects. Next, and to the extent possible, we present and discuss exemplary legal safeguards and examples of concrete oversight practices from different systems. We decided to include both legal safeguards and oversight

---

17 National Security Agency/ Central Intelligence Agency, «(U) SIGINT Strategy,» 2012, 2, https://edwardsnowden.com/wp-content/uploads/2013/11/2012-2016-sigint-strategy-23-feb-12.pdf.

18 Targeted surveillance or active computer network operations (i.e., getting access to datasets via hacking or disrupting computer networks, etc.) are just two prominent examples of other intelligence-gathering techniques. They are, of course, also very important, and they, too, must be subject to rigorous oversight. Due to our own resources, but also for the sake of reducing complexity, we focus only on the bulk collection of foreign communications here. Bulk collection is usually conducted by intercepting large amounts of data from fiber optic cables and radio and satellite links, but data can also be collected in bulk through hacking operations, which can be more effective in order to access data in a non-encrypted form, as opposed to data from transit links, which are usually encrypted nowadays.

19 Given that more and more people encrypt their communications, this is becoming increasingly more effective, as it allows intelligence services access data prior to their encryption. Hence, bulk equipment interference, as it is called in the United Kingdom, must also be placed on a robust legal footing and is subject to rigorous oversight. For a recent discussion on this, see: Nyst, «Regulation of Big Data Surveillance by Police and Intelligence Agencies,» 2018, https://1ing-2s14id7e20wtc8xsceyr-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Regulation-of-Big-Data-Surveillance-by-Police-and-Intelligence-Agencies.pdf.

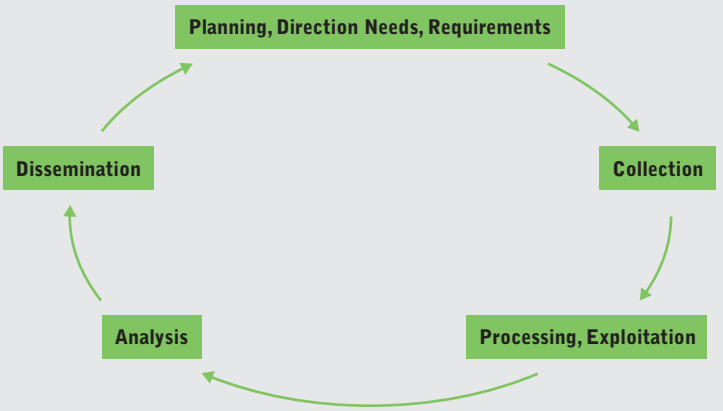
Figure 1: Bulk surveillance governance analysis scheme

practices, because they are each extremely important and mutually constitutive. Comprehensive intelligence legislation is a necessary but not sufficient condition for the effective democratic control of bulk surveillance. While not everything can be legislated,[20] one can draw, for example, on the quality of law or the strict necessity test developed by the European Court of Human Rights for some orientation on standards that modern intelligence laws ought to meet.[21] Whether or not these standards are then observed in actual practice is another story. This needs to be independently and effectively reviewed. What matters here are the actual dynamics of judicial oversight as well as its resources, legal mandate, and technological tools.

20 For reasons of source protection, e.g., national intelligence laws may not provide detailed accounts of individual tools that are to be used in the field. Others suggest that, due to the pace of technological change, it is better to adopt tech-neutral rather than tech-specific surveillance laws. Others disagree. See: Ohm, 2010.

21 As concerns the former, see, e.g., Malgieri and De Hert, «European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‹Good Enough› Oversight, Preferably but Not Necessarily by Judges,» 2017, https://papers.ssrn.com/abstract=2948270. As concerns the latter, see: Murray, Fussey, and Sunkin, «Response to Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers,» 2018, points 3–14, https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf.

Figure 2: Intelligence Cycle



For this compendium, we looked at countries with recent reforms and at places where we had access to language support and local resources. More specifically, we drew only on intelligence legislation and oversight practices from the following countries: Australia, Belgium, Canada, Denmark, France, Germany, New Zealand, Norway, Sweden, Switzerland, The Netherlands, United Kingdom, United States.

The different good practice examples in this compendium pertain to different governance dimensions, e.g. trimming the surveillance mandate, more transparency or better access to information to name just a few. For better orientation, each text boxes includes an icon. This will be further explained in the chapter IV (Discussion).

There are a number of other important caveats that readers should bear in mind before consulting our findings. First, there are many fine distinctions between targeted and non-targeted surveillance practices and the protections that are given to national and non-national data in national intelligence laws. When we run the risk of comparing things that are fundamentally different, we account for those important differences and make a case for why, as an exception, we are still drawing on a targeted surveillance regime in order to bring attention to an existing practice that, we think, should be given further consideration in bulk regimes. For example, it makes good sense to borrow from regimes on «targeted surveillance,» such as the US Section 702 program, which is meant to target only the internet and telephone communications of people

outside the United States to gather foreign intelligence information.[22] We believe that some safeguards or oversight practices that currently apply only to targeted regimes are equally suitable for bulk collection because they, too, involve big data challenges. When we borrow from targeted collection programs, we make this explicit with the help of orange text boxes.[23]

In addition, there are important differences in the intelligence laws of countries such as the United States and Germany that further distinguish in law and oversight between international communications (e.g., where either the communication originates or ends within the territorial jurisdiction of that nation) and foreign communications (e.g., where a communication may be transiting national territory, but where neither its origin or destination are on national territory). Other countries, such as the Netherlands, do not adhere to such distinctions in their respective intelligence legislation. This, too, is borne in mind and contextualized when necessary.

Second, while helpful to identify and discuss key governance challenges, we acknowledge that our multi-stage model is too linear, in the sense that an intelligence service often combines the data collected from different gathering techniques. For example, bulk surveillance data may trigger further bulk equipment interferences, and data from bulk equipment interference may be fused with the data from bulk surveillance at different stages in the «collection.» Our model does not look into the triangulation of different digital powers of modern intelligence services.

Third, some safeguards or oversight practices that we discuss in this compendium may be relevant – or even more important – in other phases of the cycle, too. Whenever we think this is the case, we cross-reference to that phase in the discussion.

---

22 More specifically, «the U.S. government may only designate foreigners located outside of the United States as «targets» for surveillance under Section 702. However, this is not to say that this practice has no impact on Americans. Section 702 currently has more than 100,000 designated targets, and it is not just limited to terrorists or «bad guys,» but rather any foreigner whose communications might relate to the conduct of US foreign affairs, such as diplomats and officials from friendly nations, or even individuals who protest outside a US embassy, support a global human rights group, or blog about international relations. The implications of this are profound: Section 702 can monitor innocent foreigners, and in the process may sweep up the communications of the average Americans they are talking to. Laperruque, «After ‹Foreign Surveillance› Law, Congress Must Demand Answers from Intelligence Community,» The Hill, January 2018, https://thehill.com/opinion/cybersecurity/370271-after-foreign-surveillance-law-congress-must-demand-answersfrom. See also: Human Rights Watch, «Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act,» September 14, 2017, https://www.hrw.org/news/2017/09/14/q-us-warrantlesssurveillance-under-section-702-foreign-intelligence-surveillance.

23 For example, we know that the US Foreign Intelligence Surveillance Court (FISC) has no role at all in overseeing bulk collection now that the Section 215 bulk collection program was ended in the USA Freedom Act. Therefore, when we single out a practice that involves the US FISC, we are mentioning a practice that relates to a targeted collection effort. While the law makes a very clear distinction between bulk and targeted surveillance, we propose here that these lines are not that clear in actual intelligence practice and that the debate on the governance of bulk surveillance should borrow good practices from neighboring regimes when possible.

III. Best Practice Compendium

Phase 1: Strategic Planning

Every government's resources are limited, and legal rules may prevent the collection of data regarding certain aspects of life. Human rights obligations or constitutional provisions prohibit or limit the collection of data in certain situations, for example when the privacy of the home is concerned.[24]

Intelligence services may also not be able to effectively process too much information, and therefore need to focus their activities.[25] Such factors require that governments set political and strategic priorities and determine the specific assignments of their intelligence community. The first phase of the SIGINT process thus involves the identification and formulation of certain intelligence needs. Ideally, strategic planning will also draw on insights from previous assessments of collected intelligence and their value after analysis.

Relevant aspects

A clear and specific legal mandate is the precondition for the transparency and accountability of foreign intelligence gathering. The mandate should describe specific legal grounds, against which the permissibility and proportionality of a particular measure can be assessed. It should also stipulate what data sources or types of communications may and may not be included in SIGINT collection.

According to jurisprudence by the European Court of Human Rights and the Court of Justice of the European Union, bulk surveillance is only permissible when it is strictly necessary to protect the democratic institutions of society.[26] This indicates that intelligence services of signatory countries of the European Convention of Human Rights and the European Union Charter of Fundamental Rights may only engage in bulk collection techniques in relation to clearly confined categories of serious threats

24 In Germany, for instance, the privacy of the home is protected by Article 13 of the Grundgesetz (Basic Law).

25 There is evidence suggesting that an overflow of data might cause intelligence failures: Gallagher, «Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure,» June 7, 2016, https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/.

26 This was established both by the European Court of Human Rights (ECtHR) and the Court of Justice of European Union (CJEU). See, e.g.: ECtHR and Council of Europe judgment in Klass and Others v. Germany, Application No. 5029/71, September 6, 1978, para. 42; ECtHR judgment in Szabo and Vissy v. Hungary, Application No. 37138/14, January 12, 2016, para. 73; CJEU judgment in Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others, Cases C-203/15, C-698/15, December 21, 2016, paras. 108, 110, 116.

to a democratic society. These categories ought to go beyond a general understanding of what constitutes a serious threat.[27]

The actors involved in setting intelligence priorities play a significant role here. There may be both external planning and tasking by government officials or ministers outside the service, and internal planning and tasking by the services. External planning and tasking traditionally focus more on a strategic/political level, whereas internal planning typically includes a stipulation of data sources or types of communications.

Who can influence and challenge the tasking process? Does an evaluation of previous intelligence cycles feed into the planning of future intelligence collection? If so, how? When it comes to the formulation of concrete intelligence needs, does the process allow those with adversarial positions to challenge what may be taken for granted? Matters concerning cooperation with foreign intelligence agencies must also be addressed at this stage: Will the need for cooperation with foreign services be weighed against other factors, such as human rights obligations and other national security interests? If so, how?

Good practice in legal safeguards

Ending discrimination based on citizenship

The majority of foreign intelligence laws are structured along a basic separation between «domestic» and «foreign» data. Domestic communication – defined either according to citizenship or based on territoriality – typically enjoys greater protection in most countries than what is seen as «foreign» or «overseas» communications. Though, as many authors have rightly pointed out, this distinction is problematic, both from a legal and from a technological perspective: As regards the latter, in a global digitized environment, it is very difficult to distinguish accurately between national and non-national data. Unless the filter programs work with 100 percent precision, incidental collection of domestic data appears inevitable. No foreign intelligence service can know in advance whether national data will be swept up in its bulk collection activities.

There is comprehensive evidence that suggests that no filter system can sufficiently sort out domestic communications from an internet data stream.[28] Even communications that are sent and received within the same country can be routed via third countries. The technical features of packet-based transmissions of communications on the internet make it practically impossible to clearly encircle a complex data category such as «German citizen.» Even if filters were to attain approximately 99 percent accuracy, in the sphere of bulk collection, where millions of communications

27 Murray, Fussey, and Sunkin, 2018, 3, point 9, https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf.

28 For a recent discussion on the accuracy of data minimization programs, see: Rechthien, 2016, and Dreo Rodosek, «Sachverständigengutachten. Beweisbeschluss SV-13, 1. Untersuchungsausschuss der 18. Wahlperiode,» 2016, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisation_rodosek.pdf.

are intercepted indiscriminately, such a small percentage of wrongly categorized communications data amounts to large-scale infringements of the right to privacy of thousands of people. Consequently, poorly documented and designed filter systems do not assuage concerns about the chilling effects and the possible rights violations. What is more, separating populations may conflict with the principle of non-discrimination, as laid down in some national constitutions, EU law, as well as in international human rights law.[29] In addition, although international law may not explicitly prohibit suspicionless bulk surveillance, it does not endorse it either. Democracies such as Germany also have an obligation to interpret its national laws with a view to their compatibility with international law. This includes the right to privacy under Article 17 of the International Covenant on Political and Social Rights (ICCPR), which, many people argue, cannot be construed as a club good.[30]

The Netherlands:
No discrimination between foreign and domestic data in intelligence collection

The Dutch intelligence law does not differentiate between national and foreign communications, thereby granting the same privacy protections to all. Given the unresolved technical challenge to accurately distinguish between national and non-national communications data, let alone the constitutional and human rights challenges to such an approach, this appears to be the most consistent and rights-based solution to the problem.

Avoiding discrimination based on citizenship in national intelligence laws does entail the risk, however, that a lower standard of privacy protections will be adopted for both citizens and non-citizens alike. This is simply because equalizing safeguards on a lower level appears to be easier and would allow for broader data collection than if the bar were raised for all. Ideally, national intelligence laws will aim for the highest possible protection for all communications data collection, regardless of the citizenship of the population under surveillance.

The German intelligence law did not do away with discrimination based on nationality in foreign intelligence collection. However, German legislators created

29 E.g., Schaller, 2018, 944.

30 Yet, there may, of course, be variations in the way in which this right may be enforced domestically. For example, a Colombian citizen may not have the same expectations of being notified that his or her communications data was intercepted by the German foreign intelligence service. More information on the topic of citizenship in national surveillance legislation can be found in: Swire, Woo, and Desai, «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft),» 2018 (arguing for nationality as a key factor in surveillance laws) and the case against the German federal intelligence law recently brought to the German Constitutional Court (in German, see: https://freiheitsrechte.org/home/wpcontent/uploads/2018/01/GFF_Verfassungsbeschwerde_BNDG_anonym.pdf).

higher privacy protection standards for European Union data, as compared to the foreign intelligence collection rules regarding non-European Union data. The BND Act (Section 6 (3) in conjunction with Section 9 (2) and (5)) establishes that the use of selectors which target public bodies of EU member states or EU institutions is restricted to 12 warranted cases and requires orders that mention the individual search terms. The use of selectors that target EU citizens is restricted to 21 warranted cases.[31] This demonstrates the willingness to grant higher levels of privacy protections, at least for European neighbors.

Legitimate criticism has been raised against the compromise made in German law, because it does not fulfill the standard of non-discrimination and ignores the issues of technical feasibility, as described above. Though, taking the realities of modern surveillance practices into account,[32] introducing additional safeguards for certain foreign populations softens the traditional dichotomy of «us» versus «them»; and by blurring this line, it can be seen as a pragmatic step forward.

Clear rules for setting intelligence priorities

United States:
Additional efforts to restrict the use of bulk powers

Presidential Policy Directive 28 (PPD 28) requires the US government to prioritize targeted collection over bulk collection, if targeted surveillance will achieve the desired results. Section 1 states that «[s]ignals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.»

Notice that PPD 28 is only an executive decree and not enshrined in statute. A US president can, therefore, change it unilaterally. In the absence of change, however, PPD 28 is binding on the executive branch. As such, these basic principles can limit the use of bulk powers. The Dutch government also proposed a policy rule that special powers have to be applied in as targeted a manner as possible.[33] Arguably, the services are already bound by the general principle of proportionality, but introducing such a requirement in the intelligence law adds an accountability dimension and reinforces

31 For a more detailed analysis of the four different standards, see: Wetzling, «New Rules for SIGINT Collection in Germany: A Look at the Recent Reform,» June 23, 2017, https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

32 Lubin, 2017.

33 Article 29, Dutch Act on the Intelligence and Security Services 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017), http://wetten.overheid.nl/BWBR0039896/2018-05-01 .

the need to deploy bulk collection methods only when less intrusive means are not able to achieve a given objective.[34] The new Dutch authorization body, TIB (Review Board for the Use of Powers), is requested to include the as-focused-as-possible principle in its regularity review, and the Dutch review body, CTIVD (Oversight Committee for the Intelligence and Security Services), is tasked to report on this.

Germany:
Transparency on actors involved in formulating the National Intelligence Priority Framework

Section 6 (1, number 3) of the German BND Act accounts for the actors that can formulate needs for the future tasking of the foreign intelligence service's signals intelligence. According to this, the Federal Chancellery determines the National Intelligence Priority Framework (Auftragsprofil BND) in consultation with the foreign office, the home office, as well as the ministries for defense, economy, and international cooperation.

United States:
Annual review of any intelligence priorities by heads of departments

Section 3 of PPD 28 requires all competent department heads to «review any priorities or requirements identified by their departments or agencies and advise the Director of National Intelligence [DNI] whether each should be maintained.»

Such a requirement for periodic review constitutes an important measure to ensure the timeliness and relevance of intelligence priorities. It also creates public accountability dimensions for key stakeholders in the intelligence policy-making process. The annual review is conducted within the executive branch only; no input from actors outside the corridors of power must be taken into account. Similarly, albeit not in statute, the Intelligence Community Directive 204 states how the National Intelligence Priorities Framework is established in the United States.[35]

34 The «as targeted as possible» criterion is part of an adopted parliamentary motion and the policy rules issued in April 2017. It is also included in a draft legislative proposal changing the ISS Act 2017. For more information, see: Houwing, «The Wiv 2017. A Critical Contemplation of the Act in an International Context,» 2018, 17, https://www.burojansen.nl/pdf/2018-LotteHouwing-WivCriticalContemplation_final.pdf.

35 US National Intelligence Priorities Framework, ICD 204, see: https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework. pdf.

The Netherlands:
Adequacy review of foreign cooperation partners

In order to assess which countries the services can share information with, weighting notes are drawn up on cooperation partners. These notes must be kept up to date and provide information on the basis of five criteria provided in law:

- the «democratic embedding» of the intelligence and security services in the country concerned;
- the respect for human rights in the country concerned;
- the professionalism and reliability of the service concerned;
- the legal powers and capabilities of the service in the country concerned;
- the level of data protection maintained by the service concerned.[36]

Planning intelligence needs involves laying sound legal groundwork for intelligence cooperation. Based on the five criteria listed above, Dutch intelligence services have to submit a weighting note for each foreign partner service they cooperate with. The weighting process requires several compulsory risk assessments on the basis of such notes.[37] In addition, the pertinent policy rules from April 2018 state that unevaluated data from bulk cable interceptions may not be exchanged without the existence of a weighting note that covers this type of exchange.[38] Put differently, in the absence of a weighting note for such a case, no sharing of unevaluated data can be authorized by the responsible minister. The Dutch oversight body CTIVD can review the notes and

36 Eijkman, Eijk, and Schaik, «Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?,» 2018, 31; see also: Dutch Act on the Intelligence and Security Services 2017, Articles 88–90.

37 In these weighting notes, the government assesses how far cooperation with a foreign service may go. If there are developments in the country of the foreign service that give rise to a revision of the cooperation, the weighting note will be revised. The Dutch government does not exclude cooperation in advance with countries that do not meet the criteria, even if there are limited democratic safeguards and a poor human rights situation. In that case, the government speaks of a «risk service.» In case of cooperation with a «risk security service,» additional permission from the competent minister is required. The weighting of cooperation with these countries and these types of risk services must always be submitted to the minister. More background on Dutch Weighting notes: Dutch Review Committee on the Intelligence and Security Service (CTIVD), «Review Report on the Implementation of Cooperation Criteria by the AIVD and the MIVD,» 2016, https://english.ctivd.nl/documents/review-reports/2016/12/22/index48.

38 However, when it comes to sharing unevaluated data that stems from other specials powers (such as targeted interception or computer network exploitation), this rules does not apply. This data can be exchanged without the existence of a weighting on the basis of Article 64 ISS Act 2017, provided there is an urgent and important reason for this.

report to parliament whether it found them to be correct and adequate (see oversight practices section below). This is an innovative way to assess which countries intelligence can be shared with. Supposedly, other intelligence agencies weigh similar factors and make their decisions accordingly, but when writing this into the intelligence legislation, it underlines the importance of appropriate weighting, and it allows oversight bodies to review the process.

Germany:
Written agreements on the aims, the nature, and the duration of international cooperation must be approved by the Chancellery

Aiming for greater accountability for international intelligence cooperation, Germany has introduced new criteria for adopting bilateral agreements between intelligence services.

According to Section 13 of the BND Act, all cooperation agreements involving bulk SIGINT on foreign-foreign communications between Germany and EU, NATO, and European Economic Area countries require a prior written memorandum of understanding (MoU)[39] and approval from the Chancellery.[40] A list of broad permissible goals for such cooperations is included in Section 13 (4) of the law.[41] The executive is required to inform the parliamentary intelligence oversight body about all such agreements. This also includes an appropriations clause that the data may only be used for the purpose it was collected, and that the use of the data must respect fundamental rule of law principles. Agreements also require a consultation among the foreign cooperation partners to comply with a data deletion request by the German Federal Intelligence Service (BND). In the end, though, due to the lack of an international arrangement, German intelligence officials cannot verify the accuracy of the assurances they may get from their cooperation partners in this regard.

Explicit mention of objectives that may not be advanced through bulk collection

Many recent reforms of SIGINT legislation have shied away from setting effective limits to bulk collection. That the United States has ended «about collection» and rolled back the bulk collection of telephone records under Section 215 of the Patriot Act in

39 One SIGINT MoU that was made public as part of the Snowden revelations is the US-Israel MoU. It is available at: https://upload.wikimedia.org/wikipedia/commons/4/41/Israel_Memorandum_of_Understanding_SIGINT.pdf.

40 Agreements with foreign partners further afield require the approval of the Head of the Chancellery.

41 Wetzling, «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls,» 2017, 13–16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

2015 is a notable exception to that rule. It proves that liberal democracies can do away with excessive collection practices. Some less prominent examples of new intelligence laws that have further restricted or trimmed the permissible use of bulk powers include the following:

Germany:
Prohibition of economic espionage

Section 6 (5) of the BND Act prohibits the use of foreign-foreign strategic surveillance to obtain economic advantages («*Wirtschaftsspionage*»).[42]

United States:
Prohibition of discrimination against protected classes through bulk collection

«In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section» (Section 2 PPD 28).

United States:
Criminal liability for willful real-time surveillance conducted for an unlawful purpose

The criminal wiretapping statute contains a prohibition to engage in real-time surveillance (18 U.S. Code 2511 (1)). The provision bans certain wiretapping activity, and then creates exceptions to that general prohibition. Section 2511(4) exempts from this criminal statute lawful intelligence surveillance activity. But intelligence officials who conduct unlawful wiretapping are committing a crime.

42 It is important to note that this provision, in general, does not preclude the German intelligence services from targeting private organizations, such as corporations. The provision has been criticized as blurry and «poorly crafted» for the lack of proper legal definition of the term «economic espionage»: Graulich, «Reform des Gesetzes über den Nachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation,» 2017, 46, https://kripoz.de/wp-content/uploads/2017/01/graulich-reform-des-gesetzes-ueber-den-bundesnachrichtendienst.pdf.

Criminalizing certain forms of intelligence surveillance deters the misuse of surveillance powers. The penalty for intentional violations against the prohibition of real-time surveillance in the US wiretapping act may range up to five years imprisonment (18 U.S. Code 2511(4)). Such criminal liabilities are rarely found in the realm of bulk surveillance, but they could be an effective means to enforce compliance with regulations.

Good practices in oversight

Setting strategic goals and formulating operational priorities is a core competence of the executive. Consequently, we found only very limited involvement of oversight bodies in the tasking and planning phases. Privacy International also found recently that no intelligence oversight body currently possesses the power to authorize decisions to share intelligence.[43] Clearly, this invokes not just legal and operational questions but also political ones. Can a government sufficiently trust a foreign service to engage in new cooperations? Interestingly, some oversight bodies have recently taken an interest in reviewing the tasking of and cooperation between intelligence services, as the following examples illustrate.

Oversight involvement in tasking

United Kingdom:
Parliamentary committee must be informed regularly about operational purposes

Section 142 of the Investigatory Powers Act details the procedure for specifying operational purposes for bulk interception. Any operational purposes must be approved by the Secretary of State (142 (6)) and must go beyond what is already prescribed in law (142 (7)). Every three months, «the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament» (142 (8)). «The Prime Minister must review the list of operational purposes at least once a year» (142 (10)).

Keeping oversight bodies regularly informed about operational purposes in actual practice helps them to identify shifting priorities and assess their compatibility with the legal framework. Thus, having a legal statute that prescribes detailed purposes or uses for bulk powers is one thing. Better still is to add actual reports on how priorities have been set in practice.

43 Privacy International, «Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards,» 2018, https://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global.

Canada:
Full access to documentation of cooperation agreements

The Commissioner of the Communications Security Establishment (CSE) can access all relevant information about the intelligence-sharing activities of the CSE. The CSE Commissioner has all the powers of a Commissioner under Part II of the Inquiries Act, including the power of subpoena, which gives CSE Commissioner and staff unfettered access to all CSE facilities, documents and personnel.[44]

The Netherlands:
The CTIVD can review the weighting notes

The Dutch Review Committee, the CTIVD, has the power to review the weighting notes on international cooperation partners and the subsequent international cooperation, as such. The CTIVD also has to be informed of any exchange of unevaluated data.[45]

Germany:
Parliamentary oversight committee must be informed about all MoUs

Section 13 (5) of the BND Act requires the government to inform the parliamentary intelligence oversight body, the Parliamentary Control Panel (PKGr), about all the MoUs signed concerning bulk SIGINT cooperation with foreign partners. This does not include ad hoc SIGINT cooperation on foreign intelligence collection.

44 Should Bill C-59 pass, the creation of a single agency to review national security activities across government departments and agencies should resolve the single focus on the CSE in this regard; see also Privacy International, 2018, 67.

45 The obligation to inform was broadened by policy rules. The law itself stipulates that the CTIVD has to be informed of unevaluated data from bulk SIGINT interception.

The three practices above are attempts to tackle the «accountability deficit»[46] of international intelligence cooperation. Unrestricted access to all cooperation agreements is a crucial step for oversight bodies to gain a better understanding of the scope and nature of intelligence-sharing. In a 2016 report, the CTIVD publicly criticized some of the services conclusions: «In one case, the foreign service does not meet the criteria of democratic anchorage, professionalism and reliability and reciprocity. Nevertheless, the MIVD [Military Intelligence and Security Service] determined that all forms of cooperation are permitted. [...] The CTIVD is of the opinion that the contents of the weighting note cannot support this conclusion. The MIVD does not indicate which compelling reasons are regarded by the service as a basis for being able to go so far in the cooperation, despite the failure to meet certain cooperation criteria.»[47] This example shows that the CTIVD may even publicly disagree with the services› weighting conclusions.

Summary of findings and reform agenda

The practices discussed in this phase comprise fundamental aspects (such as the Dutch practice to do away with the discrimination based on citizenship in bulk surveillance) to smaller, more incremental steps toward improved accountability (such as the introduction of concrete ministerial responsibilities for the steering of bulk surveillance processes).

It is noteworthy how international cooperation plays a significant role in this phase. Especially in the SIGINT world, where burden-sharing among foreign partners is a fundamental feature, weighting notes and improved access of oversight to international intelligence-sharing agreements are laudable practices. Ideally, they should be linked to mandatory and regular reevaluation by oversight bodies. The explicit mention in legislation of objectives that may not be advanced through bulk collection is another crucial dimension in shaping better governance.

Phase 2: Application Process («Warrantry»)

With a warrant, the intelligence service (or, as the case may be, the ministry performing executive control over a particular intelligence service) submits an application for authorization to collect data in bulk. Warrants need to describe and delimit bulk SIGINT measures based on specific criteria regarding both the form and content of the warrant that are set out in law. Warrants are a core element of accountability in intelligence governance, although they have to provide detail and particularity in order to constitute an effective safeguard against overly intrusive surveillance authorities.[48]

46 Bos-Ollermann, «Mass Surveillance and Oversight,» 2017, 152.

47 CTIVD, 2016, 32.

48 Donohue interviewed by Farrell, «America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?,» June 14, 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/?noredirect=on&utm_term=.2f3ee3b71c69.

In the SIGINT world, warrants might therefore be tied to classes of individuals or activities rather than specific persons. We are aware that some jurisdictions apply much stricter limits to the legal concept of a warrant. In the United States and Canada, for instance, warrants always refer to targeted surveillance operations that involve a judge, who has to authorize them. A range of countries in Europe only apply the concept of warrants to criminal investigations and not to intelligence collection. In this conventional understanding, «bulk powers are irreconcilable with the requirements of classic warrants. There is no specificity. By definition, bulk powers are not targeted; they are indiscriminate.»[49] Under the United Kingdom's Investigatory Powers Act, on the other hand, the term «warrant» is used for different types of applications for bulk interception or acquisition of data. This, then, implies a class-based warrantry system, in which large categories of data can be collected.

Although terminology is tricky and warrants for untargeted collection or bulk surveillance are not a feature of some legal systems, they are included here as a useful comparative category. Warrants can be a powerful tool to specify the minimization rules, the authorization requirements, and the purpose limitations of a measure. The more specificity a bulk warrant can provide, the better its protective function. Warrants may also be used to exclude certain data categories from collection and limit the use of the data collected.

It is important to note that many such limits and conditions could appear in a law governing intelligence surveillance. The major advantage of warrants, though, is the active involvement of an independent judicial authorization body *before* the collection begins (see phase 3), which allows for case-by-case controls. Ideally, a clear legal mandate is combined with obligatory, independent, ex-ante controls of all applications for bulk data collection.

Warrants also often define the duration of an operation for a specific collection method. This, in turn, triggers a mandatory reassessment of the measure, and potentially the subsequent reapplication and reauthorization. Setting an expiration date is, hence, an accountability mechanism as well as a regular efficacy test that helps to ensure the efficient allocation of resources by the agencies.

Naturally, the more targeted an envisaged surveillance operation, the more specific the warrant can be formulated. Given the focus of this study, that is, safeguards and oversight innovation regarding non-targeted communications surveillance, we mostly reviewed types of «bulk» warrants. This said, interesting features in targeted surveillance warrants might be discussed when applicable to the sphere of untargeted collection.

49 Forcese, 2018, 3.

It is common for various intelligence laws to include a list of criteria that each application for a SIGINT measure needs to address.[50] Ideally, these include the:

- purpose(s) of the requested activity;
- alternative means available;
- private companies that may be compelled to cooperate;
- service or services that will be instructed to perform the activity;
- time frame for assessment and authorization of the warrant, including for emergency situations;
- geographical zones or organizations or groups of people that a particular measure is directed at;
- technical device or facility to be tapped;
- exploratory monitoring or preliminary aptitude tests that have been conducted in preparation;
- type(s) of data to be retrieved;
- search terms or selectors used (i.e., a range of IP addresses);
- types of data use and forms of data exploitation to be performed on the data;
- duration of the warrant and rules for renewal;
- additional background materials to be submitted with the warrant.

Dimensions of SIGINT warrants

The following table provides examples of different types of warrants that exist in different jurisdictions. It is by no means a comprehensive list. It demonstrates, however, the diversity of different uses and applications for SIGINT warrants. The types of bulk warrants are illustrated with reference to only one legal regime, but similar provisions may exist in other intelligence laws as well. In general, the different warrants identified illustrate two things: First, warrants may be required for different collection *methods*, that is, detailing the techniques that can be used to obtain communications data. Second, many intelligence laws now require separate warrants for different *stages* of the SIGINT process. For example, the Dutch have now adopted a three-stage process that requires warrants for 1) the collection and filtering (Article 48), 2) the pre-treatment of the unevaluated data (Article 49),[51] and 3) the selection of content for operational use

50 For example, a coalition of civil society, industry, and international experts has formulated a list of 13 principles to meet the human rights obligations in relation to communications surveillance: Necessary and Proportionate Coalition, «Necessary & Proportionate. International Principles on the Application of Human Rights to Communications Surveillance,» May 2014, http://necessaryandproportionate.org/principles.

51 The pre-treatment phase (Article 49 of the Dutch intelligence Act) exists to then either improve the collection (Article 49 (1)) or to improve the selection (Article 49 (2)).

and automated data analyses (Article 50).[52] Moreover, warrants are used to regulate the retention of data, the sharing of data, and even the use of data for experiments and training. Although a specific bulk warrant must be viewed within the broader legal framework in the respective country, the table shows that various legislators have found versatile applications for bulk warrants. This, too, helps to hold the executive accountable for specific intelligence activities.

Table 1: SIGINT warrants

Type of warrant	Example provision
Bulk interception	United Kingdom: «Bulk Interception Warrants» (Section 136 (1) IP Act)
Bulk acquisition	United Kingdom: «Bulk Acquisition Warrants» (Section 158 (5) IP Act)
Bulk personal datasets	United Kingdom: «Bulk Personal Datasets Warrants» (Section 199 (1) IP Act)
Data examination	France: «Data Exploitation Warrant» (Article L. 854-2.-III. of Law No. 2015-1556)[53]
Retention	United Kingdom: «Retention notice» that orders an operator to retain communications data (Section 87 (1) IP Act)
Metadata analysis	France: The prime minister has the power to authorize, on request, the «Exploitation of non-individualized connection data.»[54] (Article L. 854-2.-II. of Law No. 2015-1556)
Operational support	The Netherlands: The Dutch services need to obtain operational support permission, in case no formal cooperation agreement exists, as if they were applying the powers themselves. «Granted permission then makes exercise of the special powers abroad as covered by Dutch law.»[55] (Article 90 Intelligence and Security Services Act 2017)[56]

52 Dutch Act on the Intelligence and Security Services 2017; see also: Eijkman, Eijk, and Schaik, 2018, 22.

53 In French original «exploitation de communications […] interceptée.» A similar type of examination warrant is, e.g., required in UK law: «An intelligence service may not exercise a power to examine a bulk personal dataset retained by it unless the examination is authorised by a warrant under this Part» (Section 200 (2) United Kingdom, Investigatory Powers Act 2016). In other cases, the conduct authorized by a bulk warrant includes safeguards on selection for examination and disclosure.

54 In French original «l'exploitation non individualisée des donnés de connexion interceptée.»

55 Ibid.

56 A similar type of warrant is also foreseen in New Zealand's intelligence law: «An intelligence and security agency may not, without an authorisation, request a government of, or an entity in, another jurisdiction to carry out an activity that would be an unlawful activity if it were carried out by the intelligence and security agency.» (Intelligence and Security Act 2017 (2017/10) Section 49 1A).

Type of warrant	Example provision
Testing	New Zealand: «A testing warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity that is necessary to test, maintain, or develop the capability of the agency in relation to the performance of its statutory functions.» (Intelligence and Security Act 2017 (2017/10) Section 91A)
Training	New Zealand: «A training warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity that is necessary to train employees in relation to the performance of the agency's statutory functions.» (Intelligence and Security Act 2017 (2017/10) Section 91B)

Doubts have been raised, though, about whether having warrants for separate stages of the intelligence process is feasible in practice. Problems might occur if the warranted phases outlined in law do not correspond to the actual consecutive steps that have to be taken. In the Dutch case, experts claim that the three steps that must be authorized are closely interrelated and run in parallel.[57] This, they argue, could mean that different warrants for separate stages of the process would, in practice, not be authorized one after the other, but in fact all at once, thereby potentially undermining the purpose of this separation.

Good practice in legal safeguards

Naturally, the level of granularity in the criteria for bulk warrants differs from country to country. Several examples stand out for their attention to important details.

Legal specifications of SIGINT warrants

France:
Restriction on the number of agencies allowed to use the data

According to the French foreign intelligence law, only the services named in the warrant are allowed to process the collected data. This specification is a protection against subsequent interagency data-sharing. Furthermore, the provision determines that the purpose stated in the warrant may not be changed, and the data may not be used for other purposes.[58]

57 See Electrospaces.net. «Collection of Domestic Phone Records under the USA Freedom Act,» July 14, 2018, https://electrospaces.blogspot.com/2018/07/collection-of-domestic-phone-records.html; CTIVD opinion: «Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX,» August 26, 2015, https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel.

58 Article L. 854-6. of French Law No. 2015-1556 on international surveillance.

This rule limits unforeseen spillovers of collected data from one intelligence service to another. Other agencies that may develop an interest in the collected data are prevented from performing unwarranted «searches on top of searches»[59] with such a requirement.

France:
Type of automated processing accounted for in warrants

Warrants for foreign-foreign intelligence must include the type of automated processing that can be implemented, specifying its purpose.[60]

Stating exactly how a bulk dataset is processed and exploited may enable reviewers to better assess the privacy intrusions that are generated by the respective operation. The level of privacy intrusions and the effects on other fundamental rights may differ based on what kind of examination is performed, and for what aim. In France, however, such applications for the exploitation of bulk metadata are authorized by the French prime minister and not independently reviewed by an oversight body.

Canada:
Specific requirements to make the «intelligence case» in a bulk SIGINT application

The proposed CSE Act (Section 35 (2) (b) as foreseen in Bill C-59)[61] requires the Canadian foreign intelligence service (CSE) to *independently demonstrate* in their application why the information to be acquired in bulk (in Canadian terms: unselected information) «could not reasonably be acquired by other means» – that is, to demonstrate why less intrusive collection methods are insufficient.

Codifying such a specification in law (as opposed to an executive decree) is prima facie a much stronger safeguard, because governments cannot change it at will.[62]

59 Renan, «The Fourth Amendment as Administrative Governance,» May 2016, 1068, http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2016/06/68_Renan_-_68_Stan._L._Rev._1039.pdf.

60 Article L. 854-2.-II. of French Law No. 2015-1556 on international surveillance.

61 All provisions referring to the Canadian Bill C-59, deal with the draft law as it exists at the time of writing: after first reading in the House of Commons, online: http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading.

62 By comparison, the German BND Act (§6 (7)) merely states that a secret service regulation will determine the specifics of the authorization process. In the United Kingdom, IPCO has recently published an advisory note (01/2018) on how it wants to review warrants, which is discussed in the section on oversight.

Naturally, lawmakers are not immune to adopting underwhelming provisions, which, once adopted, are also harder to change. Another advantage with codified provisions is that the public can have more trust in the rigorousness of the proportionality check, and the authorization body has a firm right to a more detailed explanation by the services. In Switzerland, similarly, the law explicitly demands that warrants for bulk surveillance must contain an explanation of necessity.[63]

Germany:
Listing of search terms in untargeted communications data surveillance warrants[64]

Warrants covering foreign-foreign strategic surveillance relating to EU institutions and public bodies of EU member states must specify the search terms to be used (Section 9 (2) German BND Act).

Having to specify search terms in advance is an incentive for analysts to narrow down what is relevant and to use more restrictive terms. This helps to limit the number of persons affected by the collection and avoids the risk of having to obtain a new warrant because a use of broad terms returned too many records to be useful for analysis. What is more, subsequent judicial reviews of the SIGINT practice are far more meaningful with actual knowledge of the search terms used.

The Netherlands:
Predefining specific fiber optic cables to be intercepted

The explanatory memorandum of the Dutch government noted that warrants should typically specify what (fiber) cables are to be intercepted.[65]

Stipulating the concrete technical infrastructure that is to be intercepted can be an important restriction. In the United States, orders issued for intelligence surveillance

63 Article 40 (1b) of Swiss Federal Intelligence Service Act (Nachrichtendienstgesetz, «Genehmigungsverfahren für Kabelaufklärung»).

64 A similar obligation to list «categories» of search terms in the Swiss Federal Intelligence Service Act (Article 40 c Nachrichtendienstgesetz, «Genehmigungsverfahren für Kabelaufklärung»)

65 Annex to the letter of the Minister of Interior regarding the Dutch intelligence law (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Bijlage bij brief Wiv 2017 en regeerakkoord), 2017, 3, https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2017/12/15/kamerbrief-over-wiv-2017-en-het-regeerakkoord/20171215+Bijlage+bij+brief+minister+BZK+over+Wiv+2017+en+regeerakkoord.pdf.

under the Foreign Intelligence Surveillance Act (FISA) must specify the device, account, or «facility» (50 U.S. Code 1805(a)) for which surveillance is to be applied. Naming a specific cable could qualify as a «facility» in that sense.[66] This can be an important aspect for assessing the proportionality of the operation in question, because fewer people might be affected if a specific access point for intercepting a certain communication stream is assigned.

Germany:
Direct ministerial responsibility for the activation of certain search terms

Section 9 (2) of the BND Act provides direct ministerial responsibility for applications involving search terms that target EU institutions or bodies of EU member states. The law requires the Federal Chancellery to be informed about SIGINT warrants and the search terms listed therein. This strengthens ministerial accountability, also retroactively, for malfeasance in steering foreign communications collection.

Selected examples of bulk warrant durations

The following table offers examples for the duration of warrants for foreign communications data collection in selected countries. In principle, the duration of a warrant should be determined with a view to the essential criteria for issuing the bulk warrant, for example the operational purpose for collecting the data in bulk. A shorter duration is called for if the relevant conditions underlying this operational purpose are likely to change within a short time period. If the conditions are stable over longer time periods, a longer warrant duration could become necessary. Introducing such normative guidelines for determining the duration of warrants could provide even greater flexibility for issuing warrants and lead to durations being determined by what is factually needed.

66 Kris and Wilson, «National Security Investigations & Prosecutions 2d,» 2012, 572f.

Table 2: Bulk warrant durations

Country	Duration time	Provision
France	12 months, renewable for 12 months	Article L. 854-2.-II. of Law No. 2015-1556 on international surveillance
Germany	9 months, renewable for 9 months 3 months, renewable for 3 months	Section 9 (3) BND Act Section 10 (5) G10 Act
The Netherlands	3 months, renewable for 3 months[67]	Section 29 Intelligence and Security Services Act 2017
United Kingdom	6 months, renewable for 6 months	Section 143 (1)(a) IP Act
Switzerland	6 months, renewable for max. 3 months at a time	Section 41 (3) ND Act

Good practice in oversight

Given that the drafting of applications for surveillance operations is typically a matter for the executive branch, our comparative review of oversight practices revealed no commendable or instructional examples that are relevant to this phase in the SIGINT governance process.

Summary of main findings and reform agenda

Warrants can open the door for detailed scrutiny of the tasking process. They allow reviewers to assess the legality and proportionality of communications data interception prior to their implementation. In some countries, the intelligence community cannot put its envisaged bulk surveillance measures into practice without judicial oversight. Unlike parliamentary oversight, which is often ex post in nature, this is a powerful means by which to rein in the executive.[68] Detailed warrants enable oversight bodies to better conduct meaningful proportionality tests and encourage agencies to be specific and efficient in their surveillance applications.

The various forms of bulk warrants that now exist in many countries highlight the potential for even broader applications of this accountability mechanism in the field of foreign communications surveillance. There is a need to think more creatively about further relevant criteria and additional aspects that add more precision to bulk warrants. For example, lawmakers could ask the executive to specify the actual use of

67 Notice, however, the three-month period mentioned in Article 29 of the Dutch Intelligence Act is a standard authorization period for special powers. Deviations can be found in Article 48 (collection, 1 year), Article 49 (search, 1 year), Article 50 (automated data analyses, 1 year).

68 Of course, there may be emergency situations where the intelligence community can be allowed to implement bulk surveillance measures without independent scrutiny. Yet, by default, it is preferable to have warrants by design; that applies when bulk warrants are warrants that are systematically checked by courts or review bodies before the measures are put into action.

minimization procedures and how the intelligence services intend to honor data-use limitations. If readers know of other safeguards in national intelligence laws regarding additional information that is required for warrants, we invite your comments. The same goes for the lack of best practice examples in the area of oversight innovation.

Phase 3: Authorization/Approval

After a warrant has been issued, the requested bulk SIGINT measure must be authorized or – as the case may be in different jurisdictions – approved by a review body that assesses the necessity and proportionality. Differences exist across nations as regards the moment when the independent judicial review process comes into play. In some countries, the competent minister or other members of the executive authorize warrants. In the United Kingdom, for example, the *authorization* of warrants is the privilege of the executive. Ministerial authorization, then, has to be *approved* by independent Judicial Commissioners. By contrast, in the German legal framework, warrants are *authorized* by bodies such as the G10 Commission or the Independent Committee.

The independent ex-ante authorization/approval of data collection is a crucial safeguard against the misuse and abuse of bulk surveillance powers.[69] The legitimacy of surveillance practice depends on the control of executive conduct from the outside. Enacting the control mechanism *prior* to implementation is crucial, because this can both deter and prevent certain actions from being taken. Independent authorization/approval also contains an important learning element, because the competent bodies can improve their controls, draw lessons from past mistakes, and then declare more assertively that certain measures are not required, or that no sufficient proof was presented.

Across many democracies, a dual system of authorization/approval has emerged that combines a judicial and an executive control function. A judicial oversight body – ideally a court – is best suited to administer a competent legal review of a bulk surveillance application. But, as several discussions with intelligence oversight practitioners have shown, the involvement of the political leadership level, for example the responsible minister or secretary of state, may also present a relevant safeguard, especially in the realm of foreign intelligence. The acceptance of a surveillance operation may go beyond legal criteria of necessity and proportionality and move into the political domain. Including political considerations, such as possible damage to diplomatic

69 «In Popescu v. Romania, the Court considered that the Romanian authority which ordered the surveillance (the prosecutor) was not independent from the executive. It stated that the authorising body must be independent and that there should either be judicial control or independent control over the issuing body's activity. Similarly, in the Iordachi and Association for European Integration and Human Rights and Ekimdzhiev cases the Court stressed that independent controls should exist at both the authorisation stage and the follow-up stage. The Court has a preference for judicial authorisation, even if, in Kennedy v. the United Kingdom, it accepted the British system of ministerial authorisation.» See: Venice Commission, «Report on the Democratic Oversight of Signals Intelligence Agencies,» 2015, para 106, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

relations with a foreign country, may add an important perspective to the authorization process.

Relevant aspects

The complexity and confidentiality of the subject matter require that the authorization body must be sufficiently qualified (e.g., a specialized court for SIGINT operations) and has to have the necessary powers and resources to conduct the authorization (e.g., access to all relevant information).[70] A fundamental requirement for an authorization/approval body is its independence. Further relevant aspects include:

- Who is involved in the authorization process?
  - How is the independence of the authorization/approval ensured? For example, unified, fully resourced authorization bodies with full access rights are far better equipped to conduct comprehensive reviews.
- When does the review take place? Prior to, or after the implementation of bulk surveillance measures?
- How does the authorization take place?
  - Are all warrants independently authorized, or does the law account for exceptions? For example, are there any exceptions for emergency procedures? If so, are they designed so that they do not unduly open up loopholes for unauthorized operations?
  - What assessment criteria are being used?
  - How explicit are the oversight bodies as regards its use of criteria to assess the legality, necessity, and proportionality in concrete practice?
  - How much time does the oversight body have to assess a warrant?
- Does the law foresee an appeal procedure?
  - Are the authorization decisions legally binding?
  - Is technical and adversarial advice incorporated into the authorization process? If so, how?

70 «The Court [...] found that ... in principle [it is] desirable to entrust supervisory control to a judge. ... Supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control.» See: ECtHR judgment in Roman Zakharov v. Russia, Application no. 47143/06, para. 275, http://hudoc.echr.coe.int/eng?i=001-159324.

- Do the warrants also account for metadata and «secondary data»[71]?
- Does the authorization take other (ongoing) surveillance measures into account when assessing a new warrant?[72]
- How is the authorization decision documented? Are there publicly available statistics on the number of rejections and total number of applications reviewed?

Good practice in legal safeguards

Margin of discretion for authorization bodies

Canada:
Option to approve a warrant with conditions

Bill C-59 envisages a rule (Part 2, Intelligence Commissioner Act, Section 21 (2 b)) that allows the Intelligence Commissioner to approve, reject, or *approve with conditions* the retention of foreign datasets. These conditions may refer to «the querying or exploitation of the foreign dataset or the retention or destruction of the dataset or of a portion of it,» and the intelligence commissioner has to «provide reasons for doing so, if he or she is satisfied that those conclusions are reasonable once the conditions are attached.»

Should Bill C-59 pass, the option to authorize with conditions will apply across the board for all intel authorizations (beyond the CSE, which is the Canadian foreign intelligence agency). In principle, this can provide oversight bodies with greater control over the implementation of surveillance measures. This could mean, for example,

71 «Secondary data» is a term that is often used in UK intelligence legislation. According to Graham Smith, it is «perhaps the most important category of data within the IP Act. It is, roughly speaking, metadata acquired under a targeted, thematic or bulk interception warrant. As such it is not subject to all the usage restrictions that apply to intercepted content. In particular, unlike for content, there is no requirement to obtain a targeted examination warrant in order to select metadata for examination by use of a selector (such as an e-mail address) referable to someone known to be in the British Islands. The broader the scope of secondary data, therefore, the more data can be accessed without a targeted examination warrant and the more of what would normally be regarded as content will be included.» Source: Smith, «Illuminating the Investigatory Powers Act,» February 22, 2018, https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html.

72 The concept of «Überwachungsgesamtrechnung» was developed by the German Federal Constitutional Court (Judgement BVerfG, of 12. April 2005 - 2 BvR 581/01). The concept departs from the premise that the authorizing body rarely, if ever, considers the entirety of other existing measures when deciding to approve a particular application. The court therefore proposed that, in order to assess the overall infringement of fundamental rights of a citizen, all ongoing surveillance measures must be taken into account when authorizing additional data collection.

setting a specific number of days before data has to be deleted, or defining specific kinds of information that must be destroyed before analysis.

Public reporting on individual authorization decisions

The Netherlands:
Mandatory public report by authorization body

The Dutch TIB commission is legally required to publish a public annual report.[73]

United States:
Option to request publication of a Foreign Intelligence Surveillance Court decision or opinion

«The Judge who authored an order, opinion, or other decision may sua sponte or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published.»[74]

As mentioned earlier, we purposely borrow some ideas from targeted collection systems when we believe that some of the specific practices or provisions can also be applied to non-targeted collection systems. In this case, publishing court decisions opens up room for debate and better public scrutiny of surveillance practice and legal interpretations of surveillance law.

United States:
Required declassification review for new legal interpretations

Section 602 (a) of the USA Freedom Act outlines a declassification requirement. «[T]he Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion

73 Eijkman, Eijk, and Schaik, 2018, 41.

74 United States Foreign Intelligence Surveillance Court (FISC), «Rules of Procedure,» November 1, 2010, rule 62, http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in Section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term ‹specific selection term,› and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.»[75]

To satisfy the needs for the protection of sources and methods, documents may also be made publicly available in redacted form.

Adversarial proceedings provide additional input legitimacy to the authorization/approval decision process

United States:
Option to request external legal opinion in authorization procedures

The FISC can «appoint an individual to serve as amicus curiae to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law.»[76] Hence, the Court has the option to engage in an adversarial proceeding when determining the legality/necessity of foreign intelligence warrants. The law explicitly requires the appointed «friend of the court» to provide «legal arguments that advance the protection of individual privacy and civil liberties.»[77]

The authorization of a surveillance operation becomes more robust if adversarial counsel is made available to the authorizing (or approving) body at the decision-making point in time. Hearing only one side of the argument invites regulatory capture. Therefore, the FISC maintains a pool of designated legal counsels, from which the Court may appoint an individual amicus curiae for a specific case. Requesting external expertise from such amici offers a fresh view on a significant or new legal matter and helps to avoid tunnel vision while enhancing the input legitimacy of the process. In Sweden, similarly, «in all proceedings before the Swedish Foreign Intelligence Court [*Försvarsunderrättelsedomstolen*], a privacy representative [*Integritesskyddsombut*]

75 Section 602 of the USA Freedom Act, https://www.congress.gov/bill/114th-congress/house-bill/2048/text.

76 50 U.S. Code §1803 (i)(2)(A); Cook, «The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty,» 2017, 543, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1960&context=aulr.

77 50 U.S. Code § 1803(i)(4)(A).

must be present, unless this would delay and compromise the operation.»[78] This representative is appointed by the government.

The mere indication that the FISC intends to appoint an amicus curiae has already proven to have had a deterrence effect on the executive branch. According to the FISA Annual Report 2017,[79] no amicus was appointed during that year. Yet, the Court considered appointing a person three times, but in all three cases, the government ultimately did not proceed with the proposed application or modified the final application «such that they did not present a novel or significant question of law, thereby obviating a requirement for consideration as to the appropriateness of appointment of amicus.»[80] This said, the opinions presented by an amicus curiae need not be «adversarial.» They may also bolster the government's argument, for example with technical aspects, as opposed to by default taking the opposite position from that of the government.[81]

Defining maximum permissible number of certain surveillance instruments

France:
Quotas for specific data collection methods

The French intelligence law sets quantitative limits for the use of specific intelligence techniques in order to end dispensable authorized warrants before approving new ones. The number of simultaneous authorizations of specific operations is limited to a fixed amount set by the prime minister at the recommendation of the French oversight body the National Commission of Control of the Intelligence Techniques (CNCTR).[82]

The French have adopted fixed quotas for certain collection methods in their governance scheme for targeted surveillance methods. The underlying logic – namely to force agencies to use or abandon existing authorized warrants instead of simply applying for new authorizations – seems to be an adequate tool to limit the use of specific

78 Lubin, 2018.

79 Administrative Office of the United States Courts, «Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017,» April 25, 2018, http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.

80 Ibid., 4.

81 Next to legal amici, there should also be technical amici that serve the court with expertise on technological questions. Thus far, no technical amici have been designated, let alone appointed contribute to a proceeding.

82 Commission nationale de contrôle des techniques de renseignement (CNCTR), «Deuxième Rapport d'activité 2017,» 2018, 37ff., https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf.

instruments. Potentially, quotas may also spur annual public debates about the set numbers. Naturally, the effectiveness of this approach hinges both on the process and the actual quotas used. Ideally, the quota-setting should be based on a transparent and verifiable process that outlines the specific need for a surveillance allowance.

The quota system applies to three types of data collection: first, to the interception of electronic communications,[83] with a quota of 3,040 in 2017; second, to the use of international mobile subscriber identity (IMSI) catchers, with a total quota of 60; and third, to the real-time collection of connection data, with a quota of 500.[84] The different relevant ministerial departments are assigned a subset of the overall quota (e.g., sub-quotas for interior, customs, defense, and other ministries) and checked on a daily basis by the GIC.[85]

Good practice in oversight

Explicit standards for proportionality assessments when approving bulk SIGINT warrants in actual practice

Explaining exactly how the necessity and proportionality test of a bulk collection warrant is conducted is crucial information for rating the thoroughness and legitimacy of the process. The United Kingdom's Investigatory Powers Commissioner's Office (IPCO) has published an Advisory Notice that provides advice and information to public authorities and to the general public as to the general approach that Judicial Commissioners will adopt under the IP Act when deciding whether to approve decisions to issue warrants.

United Kingdom:
IPCO Advisory Notice 01/2018

The Judicial Commissioners, who are in charge of approving bulk SIGINT warrants, must have regard for whether what is sought to be achieved by the warrant, authorization, or notice could reasonably be achieved by other, less intrusive means. In exercising that statutory responsibility, the Judicial Commissioners must, in particular, take into regard:

83 Article L. 852-1 of French Interior Security Act.

84 CNCTR, 2018, 37ff.

85 In France, the interception of communications data is managed by a specialized body called Groupement interministeriel de control (GIC). The GIC centralizes the referral of authorized data collection to the respective providers that hold the data. This body works under the purview of the prime minister and is also charged with controlling compliance with the quotas.

- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorization, or notice is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems and postal services;
- any other aspects of the public interest in the protection of privacy;
- additional safeguards for matters such as legal professional privilege (e.g., all for professional legal advisers) and journalistic material;
- the tests of necessity and proportionality, as applicable under the Human Rights Act 1998 and under European Union law, to the extent that this applies to the powers/activities for which approval is sought.[86]

This Advisory Notice is not binding and can theoretically change at any point in time. Therefore, it only represents the opinion of the current Judicial Commissioners, because there is also no obligation to inform the public whether the guidelines were revised. The gold standard for providing transparency remains setting out such procedural rules in law. Some critics have pointed out that the Advisory Notice has failed to emphasize «the importance of a current and relevant intelligence case justifying the decision to issue warrants,»[87] particularly in national security cases, where the Advisory Notice leans toward a wider margin of judgment.

United Kingdom:
Open oversight – civil society dialogue on proportionality standards for the review of bulk powers

Following the publication of the Advisory Notice in January 2018, IPCO proceeded to enrich these principles in May 2018 with the help of a public invitation for input on issues relevant to the proportionality of bulk powers. IPCO asked NGOs and others to provide assistance in identifying the broad range of factors that the Judicial Commissioners should have in mind when evaluating the proportionality of bulk warrants:

86 IPCO, «Advisory Notice 1/2018. Approval of Warrants, Authorisations and Notices by Judicial Commissioners,» 2018, 4, https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf.

87 The Chambers of Simon McKay, «Judicial Approval of Warrants, Authorisations and Notices under the Investigatory Powers Act 2016: A Review of the Investigatory Powers Commissioner's Office First Advisory Note,» 2018, https://simonmckay.co.uk/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/.

- What factors should the Judicial Commissioners take into account when considering whether the conduct proposed in a bulk warrant is proportionate?
- Is there any particular approach that the Commissioners should adopt when evaluating those factors, some of which may be competing?[88]

Summary of main findings and reform agenda

Independent authorization becomes an even more powerful democratic safeguard if the procedure is fully transparent and when the review officials are endowed with a robust mandate and enough discretion to authorize or approve warrants with conditions. Ideally, the legal framework stipulates a mandatory declassification review that aims to publish as much information as possible, for example about critical legal interpretations.

Adversarial proceedings are an essential feature of potent independent approval/authorization. Equally, explicit standards for proportionality assessments for authorizing or approving bulk SIGINT warrants in actual practice, such as IPCO's Advisory Notice combined with its subsequent outreach to civil society and other experts, are promising examples of good practice. If readers know about other specific standards that are being used by other oversight bodies when it comes to availing themselves of adversarial counsel or assessing the proportionality of SIGINT measures, kindly let us know. The same holds true for information on how oversight can or should verify whether a particular measure is likely to yield timely and relevant information.

Further oversight body involvement should now be considered when it comes to the authorization to share intelligence.

Phase 4: Collection & Filtering

Once a warrant has been authorized or approved, an intelligence agency can proceed with the implementation of a particular surveillance measure. For this, it intercepts the relevant signals, for example by tapping an internet service provider's (ISP) fiber optic backbone cable or diverting data at an internet exchange point. Afterwards, the collected data has to be filtered for two reasons: First, because of the huge volumes passing through, which would be far too much to be stored long-term, gratuitous data that is extremely unlikely to yield any intelligence value is filtered out (e.g., all data from public video feeds); second, the collected data stream has to be filtered so as to abide by legal requirements. Certain data – for example domestic communications or the communications involving lawyers, priests, or other professions relying on

88 IPCO, «IPC Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers,» May 23, 2018, https://www.ipco.org.uk/docs/IPC_Submissions_on_bulk_powers.pdf; the submissions can be found here: https://www.ipco.org.uk/Default.aspx?mid=4.13.

the confidentiality of correspondence – may be offered higher levels of protection in national surveillance laws.[89]

Collection

Relevant aspects

At the collection point, it is critical to clearly define who is in charge of extracting the data and where and how the extraction devices may be installed. Is the collection administered by the intelligence service, or do private entities (e.g., ISPs) do this on behalf of the intelligence services? This distinction is relevant, as provider intermediation can be an important safeguard against over-collection. In principle, intelligence agencies should not have direct access to the facilities of telecommunications providers. Cases have surfaced, though, in which internet companies agreed to search the data they administer on behalf of an agency. Yahoo, for example, secretly scanned all email accounts for information provided by US intelligence agencies.[90] A legal framework, therefore, has to define how (private) intermediaries may be compelled to cooperate and what means are available for operators to challenge particular measures.

Good practice in legal safeguards

Intermediary for centralized data collection

France:
Specialized executive body serves as data collection center

In the French intelligence community, most data collection from third parties, such as internet service providers or communication service providers such as Google and Facebook, is handled by the GIC. This body is technically not part of the intelligence community. Rather, it serves as a centralized hub that manages all data interception/acquisition under the purview of the prime minister.[91]

89 As established earlier, it is not always technically possible to filter out the communications of protected categories such as certain professions. Individuals or groups concerned could submit their phone numbers to intelligence and law enforcement agencies, but for internet communications, clear-cut filtering is much more complicated.

90 Menn, «Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources,» October 5, 2016, https://www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

91 Government of France, «Groupement Interministériel de Contrôle (GIC),» http://www.gouvernement.fr/groupement-interministeriel-de-controle-gic; «Le Groupement interministériel de contrôle va beaucoup donner,» http://defense.blogs.lavoixdunord.fr/archive/2016/02/01/groupement-interministeriel-de-controle-14495.html.

It is preferable for an intermediary body such as the GIC to be responsible for the first filter/selection process, as fewer agents will have access to the collected data. A similar specialized data collection center exists in Switzerland.[92] Consolidating all cable-tapping and data acquisition in the hands of one body may also be done for reasons of cost efficiency: Instead of having technical experts spread across the intelligence community, bundling expertise and competencies in one body may allow for the better use of the staff and resources available. Plus, it simplifies the accountability process.

Centralizing the management of data access on behalf of the agencies can also serve to facilitate holistic oversight of all the data collected. The GIC only grants analysts access to data that they need for a given assignment. This gatekeeping function may help to maintain secrecy. That said, centralizing data storage also entails the risk of creating a single point of failure for data security (e.g., hacking attacks, etc.). However, the French oversight body CNCTR describes the data intermediary as an effective safeguard, because the GIC – and not the intelligence services themselves – implement and manage the data collection.[93]

United States:
Options for providers to object to government requests for data

A private intermediary that receives an interception order under the FISA regime, such as an ISP or an internet exchange point, may challenge such an order in the FISC.[94]

One well-documented, albeit unsuccessful, objection to a government request was a 2007 Yahoo case. The service provider challenged the constitutionality of an order to hand over user information under the Protect America Act. After losing the initial challenge before the FISC, «the provider appealed the decision to the Foreign Intelligence Surveillance Court of Review.»[95]

92 The implementing data interception service is called «Zentrum für elektronische Operationen» (ZEO). See: Führungsunterstützungsbasis FUB, «ZEO (Elektronische Operationen),» https://www.vtg.admin.ch/de/organisation/fub.html.

93 CNCTR, 2018, 16.

94 One such proceeding is published (in redacted form) here: https://www.aclu.org/2014-fisc-opinion-internet-service-providers-challenge-section-702-surveillance.

95 Electronic Frontier Foundation, «Yahoo's Challenge to the Protect America Act in the Foreign Intelligence Court of Review,» October 22, 2013, https://www.eff.org/cases/yahoos-challenge-protect-america-act-foreign-intelligence-court-review; other, more recent provider challenges include: Conger, «An Unknown Tech Company Tried (and Failed) to Stop the NSA's Warrantless Spying,» June 14, 2017, https://gizmodo.com/an-unknown-tech-company-tried-and-failed-to-stop-the-1796111752.

United States:
ISPs responsible for installing splitters and selector lists

Under Section 702, private internet service providers – and not the agencies – are in charge of implementing the authorized upstream collection systems. «The government identifies or ‹tasks› certain ‹selectors,› such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition.»[96] Then, «the provider is compelled to give the communications sent to or from that selector to the government.»[97] If the agencies were in charge of the selector activation, this could lead to additional collection.[98]

Relying on a private intermediary to install and maintain the interception devices constitutes a safeguard, because the agencies cannot single-handedly reuse or misuse the devices for other aims. Intermediaries that are compelled to cooperate have an incentive to closely measure each government request against the relevant legal requirements. Internet companies have reputational costs associated with enabling far-ranging access to their customers› data and, therefore, may only allow what is strictly necessary. This additional layer of scrutiny is missing when countries give their intelligence agencies direct access to systems or communication infrastructure, with no provider serving as an intermediary.[99]

Good practice in oversight

Technical oversight interfaces for direct database access

A number of European countries (see table 3) have installed interfaces that give oversight bodies direct access to collected data. Such direct access could be an important innovation for oversight, but it also entails risks that have to be addressed.

---

96 Privacy and Civil Liberties Oversight Board (PCLOB), «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,» July 2, 2014, 7, https://www.pclob.gov/library/702-Report.pdf.

97 Ibid.

98 The public also gain some insights in the cooperation between agencies and ISPs based on an email sent from Deutsche Telekom to the BND that was published here: https://de-de.facebook.com/peterpilz/photos/902029969840817.

99 E.g., a number of EU countries (Sweden, Hungary, Romania, Estonia, Latvia, Lithuania) have direct access, and Finland is now considering direct access legislation. For more information on this, see the forthcoming paper by the Center for Democracy and Technology on the subject.

Table 3: Technical oversight interfaces

Country	Access characterization
France	«The CNCTR enjoys permanent, complete and direct access to the implementation reports and registries of surveillance techniques, to the collected intelligence, as well as to the transcriptions and extractions carried out by the intelligence services.»[100] This is based on the oversight body's direct technical interface with the GIC.
The Netherlands	«To conduct their assessment, the oversight department of the CTIVD has direct (digital) access to classified information kept by the AIVD [General Intelligence and Security Service] and MIVD.»[101]
Norway	«The Committee can carry out most of its inspections without assistance directly in the services› electronic systems.»[102]
Switzerland	AB-ND [independent supervisory authority on intelligence activities] has direct online access to the data stored by the Federal Intelligence Service (NDB), including specially protected personal data. This remote access is not permanent, but granted on a case by case basis for a specific investigation of the oversight body on a specific database.[103]

The advantage of direct access to databases is that the oversight body can conduct random checks, unannounced inspections, and potentially also automated controls on the data handling by the intelligence agencies. This has the potential to level the playing field between the controller and the controlled. Traditionally, oversight bodies depend, to a large extent, on the information provided by the intelligence services. If overseers gain direct access, the incentive to comply increases, because intelligence officials cannot know whether an incident will be reviewed or not. Technical interfaces might also empower review bodies to monitor statistical anomalies in the databases. This opens a new field of (automated) oversight applications that will support overseers in effectively diverting their limited resources for in-depth compliance auditing. Such an approach – using analytical techniques to identify potential non-compliance – amounts to «predictive oversight» and is already being practiced by institutions entrusted with financial audits in the banking sector.

Granting direct, unfettered access for oversight bodies to the intelligence databases may, however, turn them into attractive targets for foreign espionage and hacking

100 Article L. 854-9 of Law No. 2015-1556; see also: European Union Agency for Fundamental Rights, «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update,» 2017, 79, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf; see also: French Interior Security Act, Article L. 833-2.

101 Eijkman, Eijk, and Schaik, 2018, 38.

102 Norwegian Parliamentary Oversight Committee (EOS Committee), «Annual Report 2017 - Document 7:1 (2017-2018),» February 22, 2018, 10, https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.

103 Article 78 (4–5) of Swiss Federal Intelligence Service Act (Nachrichtendienstgesetz, «Aufgaben, Informationsrechte und Empfehlungen der Aufsichtsbehörde»).

attacks. It is important, therefore, to only grant such access to properly trained oversight personnel and to provide the highest level of cybersecurity to oversight bodies.

Making sense of raw intelligence data and log files is hard. It is not enough for oversight bodies to merely have access. The information advantage that direct access may bring comes from data analytics. In other words, oversight bodies need to engage with the data that they now have access to. In order to learn how much more rigorous their controlling could become, overseers may want to learn from financial audit bodies and will need special training. They may also want to commission the design and implementation of control algorithms.

Filtering

Once data has been acquired by means of untargeted electronic surveillance, it may be subject to additional filtering, depending on the national surveillance regulations.

Relevant aspects

The specifics of the data minimization and filtering processes should be subject to critical review, for they may reveal the extent to which intelligence agencies abide by constitutional and human rights standards. For example, some intelligence laws grant enhanced privacy protection to professions that depend on the confidentiality of information. This may pertain to communications involving priests, lawyers, journalists, and physicians. Whether and how data minimization and filter tools are capable of accommodating such communications in practice should be of interest to oversight bodies. This may also extend to the review of protected health data and DNA-related information.

In addition, there are technical questions that come to mind, as they, too, reveal interesting information about the independence of oversight bodies and the extent to which data minimization is an actual priority (or not) within the intelligence community. For instance, how is «surplus information» treated in the collection and filtering process? When data minimization systems, such as the Massive Volume Reduction (VRE) systems of the United Kingdom's Government Communications Headquarters (GCHQ), are being used, are they subject to independent oversight? More specifically, are the technical equipment and filter programs regularly subject to independent verification, or do the oversight bodies merely rely on the assurances of the intelligence agencies that the data minimization and filtering processes are fit for purpose?

Good practice in legal safeguards

Deletion of material that has been filtered out

The Netherlands:
All raw data (including content and metadata) that gets filtered out will be impossible to retrieve by the intelligence services

While content and metadata may be stored for up to three years (by default one year; two possible extensions of one year each) in the Netherlands, data must immediately and irretrievably be destroyed as soon as it is filtered out, or otherwise determined not to be relevant for any other intelligence investigation.[104]

The services have an obligation to assess the relevance of the data collected (see data maintenance section below).

Good practice in oversight

Review of compliance audits

United States:
The FISC reviews compliance audits performed by the intelligence community

Modern intelligence agencies should have dedicated staff for internal compliance auditing. Allowing an independent body such as the FISC to review internal audits strengthens the impact of these controls. However, the FISC relies only on the intelligence community to present audit data and does not engage in its own compliance investigations. Ideally, an oversight body would also conduct its own random sample test in order to verify the thoroughness and completeness of these compliance audits.

104 Dutch Act on the Intelligence and Security Services 2017, Article 48 (5). See also: Annex to the letter of the Minister of Interior regarding the Dutch intelligence law, 2017, 3.

A noteworthy practice is the increasing availability of technical oversight interfaces in various European countries. We also discuss the involvement of private parties (e.g., providers) and public intermediaries (such as the GIC in France) that may facilitate and centralize the collection of data. Whether the centralization of the data management and the live access to intelligence databases can be turned into an added value for oversight and democratic governance remains an open question, however. There is a need for further research as regards the effective use of such tools for different control functions.

Telecommunications providers are a central stakeholder group in the field of surveillance and, hence, must have a strong voice. Providing the possibility to substantially challenge surveillance orders is an important practice in this regard.

The independent verification of data minimization techniques deserves greater attention from oversight bodies. They ought to look into the technical implementation of the filtering process and the independent auditing of filter effectiveness. Similarly, the deletion of data is an ongoing oversight challenge that many review bodies are gradually waking up to. Here, we find that mutual learning from regular exchanges with other oversight bodies in other countries and the promotion of systematic dialogues with external experts ought to be intensified.

Phase 5: Data Processing

Once data has been collected and filtered, it must be stored, tagged, and later removed or destroyed. This phase of the SIGINT process is particularly relevant for oversight and the services because lawful and efficient data management is the basis for relevant data analysis. For the sake of clarity, this phase is divided into four subcategories reflecting the different facets of data processing: storage, maintenance, sharing, and deletion.

Data storage

Relevant aspects

Due to different retention periods, it may become necessary to keep separate databases, for example for encrypted data, metadata, and content data, or in order to distinguish data pools according to their legal basis or warranted purposes. It can therefore be relevant whether there are isolated data storage locations. Increasingly, bulk surveillance governance relies on the verifiable technical or institutional separation between the authority to intercept and the authority to analyze the data. In order to honor data protection obligations, a surveillance law should further restrict the extent to which databases may be linked or accumulated.

Transnational threats prompt closer trans-border cooperation among intelligence services, not least for neighboring countries. Intelligence data – both unevaluated and evaluated – is therefore not just shared bilaterally, but also stored in joint intelligence

databases for different threats and purposes. When we speak of *joint databases*, we refer to a multilateral exchange of data that can be hosted either on national territory or abroad. Typically, joint databases are run multilaterally, with all participating services adding and accessing data.

The European Counter Terrorism Group (CTG), for example, runs a database that facilitates the multilateral exchange of evaluated data on individuals who have traveled to and returned from certain conflict areas.[105] This database became operational in July 2016, is administered on servers in the Netherlands, and makes information available in (near) real-time to the 30 participating services of the CTG. Interestingly, unevaluated data may also be exchanged within the CTG, albeit not via the database. It may be jointly stored and processed within standard SIGINT cooperations.[106]

The CTIVD's report concludes that safeguards for the protection of fundamental rights are currently not being sufficiently addressed and recommends setting up additional safeguards and multilateral controls.

Data storage periods for «foreign» data

The table below shows exemplary data storage periods in three countries for foreign intelligence collection. Not listed are the various options for extension of storage periods, which are also provided for in the respective laws.

Table 4: Data storage periods

Country	Storage periods	Provision
Germany	Metadata: 6 months Content data: 10 years (exceptional extension possible)	Section 6 (6) BND Act Section 20 (1–2) BND Act Section 12 (3) BVerfSch Act
France	Metadata: 6 years (from their collection) Content data: 12 months from the date of first data exploitation Unevaluated content data may be stored for 4 years from the date of collection Encrypted data: 8 years	Article L. 854-5. of Law No. 2015-1556 on international surveillance

105 CTIVD, «Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD,» 2018, 10, https://english.ctivd.nl/documents/review-reports/2018/04/24/index. See also: van Eijk and Ryngaert, «Expert Opinion – Legal Basis for Multilateral Exchange of Information,» Appendix IV of CTIVD rapport no. 56 to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD, 2017, https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv.

106 CTIVD, 2018, 9.

Country	Storage periods	Provision
The Netherlands	Content and metadata after filter process: 3 years, starting after decryption Encrypted data: 3 years with *unlimited* extension possibilities for further three years	Article 48 (5–6) of the Dutch Intelligence and Security Services Act 2017

Good practice in legal safeguards

Protecting all data categories

The Netherlands:
No distinction between metadata and content data in data retention

Metadata alone – that is, information about calls and emails, for example – can reveal just as much, or even more, about a person or group as content. It is in no way less sensitive or worthy of protection than communications content.[107] On a technical level, the line between content and metadata can also be blurry and create legal uncertainties.[108]

Whereas content can be relatively easily encrypted by users, metadata such as call records and information about sender and recipient of a message is technically much harder to conceal. Due to the large quantities of data in SIGINT, the bulk of all data processing done by signals intelligence agencies concerns metadata. Consequently, many legal safeguards that only concern content fall short of effectively protecting the right to privacy. Doing away with the content vs. metadata divide in legislation therefore appears to be a laudable step toward better privacy protections.

107 Carey, «Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information,» May 16, 2016, https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/, and Bradford Franklin, «Carpenter and the End of Bulk Surveillance of Americans,» July 25, 2018, https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans.

108 Bellovin, Blaze, Landau, and Pell, «It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law,» 2016, https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf.

Germany:
Obligation to keep a file classification scheme

The BND has to keep a separate file arrangement memo for each joint database that it is responsible for (Section 28 BND Act). Therein, it must inform about the title of the database; its purpose; the conditions for retention, transfer, and use; the originator and access; the mandatory review and protocol periods; and the legal basis for creating the file. It must also provide an explicit account of foreign public authorities that are entitled to upload or download data from the database. The Chancellery needs to approve each file arrangement memo, and the German data protection authority (DPA) is to be consulted prior to the implementation.

A restriction to this rule is that the law explicitly states that the review mandate of the German DPA covers only the creation of the joint database and the data transfer from the BND to the joint database.

If a joint database with a foreign service is run by a foreign intelligence service abroad, the Chancellery needs to approve the BND's contribution to such a database, too (Section 30 BND Act). Moreover, the BND may only submit personal data to such joint databases if it is allowed to hold such data in its own databases. This is of relevance because the local DPA or review body may need to know to what extent the submissions of data from the national service to a joint database that is administered abroad are identical with the data the national service keeps in its files.[109]

Germany:
Appropriations clause for joint databases

For German services to contribute to joint databases (irrespective as to whether such a database is hosted at home or abroad), there needs to be a written MoU that covers the purpose of the database and also includes an appropriations clause. The latter requires all signatories to attest that the data cannot be used for purposes other than the ones for which they have been originally collected (Section 26 (4) BND Act).

109 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), «Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041),» September 21, 2016, https://www.bundestag.de/blob/459634/a09df397dff6584a83a43a334f3936a3/18-4-660-data.pdf.

United States:
Equalized SIGINT retention rules for US persons and non-US persons

Section 4 (a) of PPD 28 states that «[p]ersonal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons.» The general storage period is five years, with the possibility of the DNI extending that period.

Good practice in oversight

The Netherlands:
Oversight 3.0 project on future challenges run by oversight body

The CTIVD has set up a multi-year research project to better understand and address the technical challenges of intelligence oversight in the digital age.[110] These include new data acquisition techniques, the effective deletion of irrelevant or outdated data, and automated data analyses. By actively investing time and money in the exploration of new options for the oversight of digital intelligence methods, and by including scientists and other independent experts in the process, the CTIVD is laying important groundwork for the future development of oversight.

Germany:
Joint inspections of judicial oversight body and DPA[111]

In many countries, separate bodies take on different oversight functions in the SIGINT cycle. In the Netherlands, for example, there is the TIB, the CTIVD, and the parliamentary oversight committee. In Germany, bulk SIGINT is reviewed

110 CTIVD, «Start project Toezicht 3.0.,» April 25, 2017, https://www.ctivd.nl/actueel/nieuws/2017/04/25/index-2.

111 BfDI, «26. Tätigkeitsbericht 2015–2016,» 2017, 134, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=7.

by the G10 Commission and the Independent Committee. Both the federal DPA and the parliamentary oversight body also have roles to play in the democratic control of bulk surveillance.

A higher number of review bodies may mean a higher risk that important information may fall between the cracks or is not sufficiently contextualized when reviewed. Against this backdrop, the German DPA and members of the G10 Commission have begun to perform joint inspections.

Data maintenance

This comprises all practices that concern the labeling and registration of intelligence databases. Data upkeep is not only required by data protection regulations but also serves a practical end: It ensures that the services keep only relevant and accurate data.

Relevant aspects

How is bulk data tagged? And what authority do DPAs have to investigate the sound implementation of databases? For auditing purposes, data must be traceable throughout the entire lifecycle. It is also important to anonymize data to the greatest extent possible. The security and quality of the databases must be ensured to protect the sensitive information from being stolen or compromised.

Adequate data maintenance also builds on clear restrictions of data access. Is the access to the stored data regulated by law and restricted to specialized personnel only? Or is data access for operational teams limited by data exploitation warrants (see phase 2)?

Good practice in legal safeguards

The Netherlands:
Duty of care as regards data processing, including the use of algorithms

The Dutch Intelligence Act imposes a general *duty of care* upon the heads of the security and intelligence services (Section 24). It includes adequate measures against data breaches and ensures the validity and integrity of processed data. The Dutch intelligence services are also obliged to «take sufficient measures

to safeguard the quality of data processing, including the algorithms and (behavioral) models used. By covering algorithms and models, the legislator intends to take a technology-neutral approach.»[112]

The law requires all data to be examined as soon as possible to determine whether it is relevant to the operation for which it was obtained (Article 48). Data that has been determined not to be relevant shall be immediately destroyed. After one year, all data that has not been examined for relevance must also be destroyed.

Taken together, these provisions create a legal umbrella that protects the privacy and the quality of the data. The CTIVD has the competence to monitor the measures taken to this effect and to control the design of the systems deployed to comply with these duties.

Germany:
Mandatory tagging of all bulk SIGINT data

The BND Act requires the services to tag all data that is being collected (Section 10 (1)). This is an important precondition for meaningful data protection controls.

Good practice in oversight

Obligation to perform regular reviews of intelligence registration and data processing

France:
Mandatory ex-ante opinion by oversight body on the data-tagging process

The interception and exploitation of communications data are subject to tagging mechanisms that allow for tracing the subsequent data handling. The CNCTR has to submit an ex-ante opinion to the prime minister.[113] In the past, this included recommendations on metadata collection processes, retention periods,

112 Eijkman, Eijk, und Schaik, 2018, 29.
113 See: Article L. 854-4. of French Law No. 2015-1556 on international surveillance.

storage conditions, and the creation of log files.[114] Although these opinions are not binding, we find that such obligatory early involvement of the oversight body may encourage the services to address the needs of oversight while constructing the data-tagging process.

An obligation to regularly review all intelligence registrations (files, databases) would strengthen data maintenance. The Norwegian oversight body, the Parliamentary Intelligence Oversight Committee (EOS), made a proposal in that regard: «In the Committee's opinion, intelligence registrations should be reviewed periodically by the person or persons responsible for registering the information in order to ensure that the intelligence register contains up-to-date, correct, necessary and relevant information.»[115] A member of the G10 Commission formulated a similar demand, calling for mandatory data protection reviews by the G10 Commission at least every two years.[116]

Data-sharing

Relevant aspects

Sharing data with foreign services entails a responsibility to assess and mitigate the risk of misuse of the shared data. Although SIGINT burden-sharing among partner services is a common practice, what rules and procedures are in place to evaluate partner services› data quality and data veracity? Oversight of – and accountability for – data-sharing agreements and joint databases must be ensured. Finally, in times of advanced joint intelligence databases, how do oversight bodies cooperate internationally to control the permissible use of international data pools?

Good practice in legal safeguards

Different logics for oversight body access to shared data

Our comparative review reveals that oversight bodies have found different responses to the originator control policy that, supposedly, governs much of the international intelligence cooperation. Accordingly, an intelligence service may neither share the information nor the source of information it has received from a partner service with third parties without the prior consent of the entity that provided the information in the first place.

114 See: CNCTR, 2018, 16.

115 EOS Committee, 2018, 19.

116 Huber, «Kontrolle der Nachrichtendienste des Bundes – Dargestellt am Beispiel der Tätigkeit der G10-Kommission,» 2017, 15, https://beck-online.beck.de/Dokument?vpath=bibdata-%5Czeits%5CGSZ%5C2017%5Ccont%5CGSZ.2017.H01.gl2.htm.

Table 5: Access to shared data

Oversight body as «third party» General practice not to grant oversight body access to third-party data	**Oversight body with more access to third-party data** General permission with reservation to restrict access in exceptional circumstances	**Oversight body with unrestricted access to third-party data** Unrestricted access to intelligence stemming from third parties
Example country: Germany Information received from another intelligence service is, by default, not to be shared with the oversight body. However, the government is under an obligation to seek permission to do so from its cooperation partner.[117]	**Example country: Norway** In principle, the oversight body has access to all data the Norwegian intelligence service holds, including from third parties. Exceptions apply only to «particularly sensitive information.»[118]	**Example countries: Denmark and the Netherlands** Oversight bodies in these countries are not hindered by third-party restrictions and can see all the data that their intelligence service holds.

Norway:
By default, greater access to third-party information for oversight body

The EOS Committee, as a clear rule, shall have access to all information in the Intelligence Service that the committee considers relevant for its control activities. Only exceptionally, the head of the intelligence service has the right and duty to refrain from giving the committee «particularly sensitive information» and, instead, refer to the ministry of defense for further assessment of whether access is to be granted.[119]

The exception of particularly sensitive information comprises:

- The identity of the human intelligence sources of the Norwegian Intelligence Service and its foreign partners;
- The identity of foreign partners› specially protected civil servants;
- Persons with roles in, and operational plans for, occupational preparedness;

117 Wissenschaftlicher Dienst des Bundestags, «Kontrolle von Nachrichtendiensten bei Zusammenarbeit mit anderen Nachrichtendiensten im Ausland,» March 2017, 6, https://www.bundestag.de/blob/508038/5a79b26ee2205e08171ee396ef87ae45/wd-3-072-17-pdf-data.pdf.

118 EOS Committee, «Dokument 16 (2015–2016). Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget),» February 29, 2016, 71 (point 19.5, own translation), https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf.

119 Ibid.

- Foreign partners› particularly sensitive intelligence operations abroad, which, if they were to be compromised,
  - could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
  - could lead to serious injury to, or loss of life of, personnel or third parties.[120]

This does not limit the EOS Committee's insight into information about, and from, Norwegian and foreign sources per se. As a general rule, the EOS Committee has access to intelligence services› and cooperation partners› foreign operations.

Compared to other countries, such as Germany, which apply a rather strict interpretation of the third-party rule vis-à-vis their oversight bodies, the Norwegian model of oversight access to shared data offers greater control options for review bodies. Yet, as the table above also shows, there are also countries such as the Netherlands and Denmark that allow their oversight bodies unrestricted access to intelligence stemming from third parties.[121]

Good practice in oversight

Germany:
Random sample checks on automatic transfers of personal data to foreign intelligence services[122]

Regarding the automatic transfer of personal data to foreign intelligence services, the Independent Committee is authorized to perform random checks to verify that no data that violates the ban on industrial espionage (Section 6 (5) BND Act) and no other data that may counter Germany's national interest is shared (Section 15 (3) BND Act). Moreover, it can also perform random checks on the search terms that are being used for surveillance on data pertaining to EU member states or EU institutions (Section 9 (5) BND Act). Given the technical difficulties of fully ensuring that no national data is being shared (see phase 1), a review mandate for the oversight body to review such data transfers becomes even more important.

120 EOS Committee, 2018, 54.

121 Information obtained at the European Intelligence Oversight Network workshop on May 14, 2018.

122 Section 15 (3) BND Act.

Data deletion

The proper deletion of data is an enormous challenge. Technically, it is not as easy as one may think to securely «get rid» of data. This is because «deleting» a file typically only marks the space it occupies as usable. Until the disk space is overwritten, the data is still there and can be retrieved. To ensure that the deleted data cannot be retrieved any longer, the physical records on a storage medium must be overwritten with other data several times (minimum of seven times as per the US Federal government's guidelines).[123] But simply overwriting the storage space on a physical medium with new data does not necessarily guarantee that none of the old data is gone for good. Although there are technical means to ensure that deleted data is actually unretrievable,[124] it seems necessary to develop more detailed standards for what constitutes the proper deletion of data. Errors in this process could result in millions of datasets being falsely stored for years.

Moreover, it is now also «more costly to delete data, than retain it.»[125] Therefore, legislators have found it difficult to insert the proper legal definitions or public standards for what «deletion» or «destruction» of data means into intelligence laws.[126] By extension, then, the deletion problem also becomes a veritable oversight challenge. This is because review bodies need accurate audit trails to be able to check services› compliance with data deletion requirements. This may include the automated destruction of data after legal retention periods have lapsed or if the relevant authorization for collecting data has ended.

There is also a need for better guidelines on what data should be deleted at what point in time. Storage periods (see part one of phase 5 above), for that matter, define maximum times for which data may be retained. With adequate normative criteria at hand, the services or the competent oversight bodies could, theoretically, also decide to apply a shorter storage period. For example, if a system flags data that has not been used for a certain time period, this should then prompt a check as to whether this specific dataset is still needed.

Relevant aspects

Intelligence law should outline specific and short retention periods, after which the data has to be permanently and unmistakably destroyed. There might be special requirements for the data deletion of large amounts of data. For example, the NSA's

123 Dorion, «Data Deletion or Data Destruction?,» July 2008, https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction.

124 For an encryption-based approach, see: Reardon, Ritzdorf, Basin, and Capkun, «Secure Data Deletion from Persistent Media,» 2013, https://doi.org/10.1145/2508859.2516699.

125 Organisation for Economic Co-Operation and Development, «The OECD Privacy Framework,» 2013, 100, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

126 We are grateful to Professor Nico van Eijk, who presented valuable information on the legal and technical challenges of data deletion during our workshop on May 14, 2018.

XKeyscore system may have a rolling buffer, so that new incoming data automatically overwrites the old data.

It is also relevant how data destruction is documented and controlled by the competent oversight body. For example, is stored data linked to specific warrants, and does it have traceable time stamps for full and proper deletion? Adequate records of the data destruction are also important for possible notification purposes.

How are storage and deletion implemented in practice? Should intelligence data be stored in «clouds»? Even in the sphere of national security, we witness close cooperation with commercial third parties, such as private cloud storage services.[127] How can it be ensured that such outsourcing – entailing the risk of shifting responsibility for a crucial phase of data processing to private companies – does not undermine democratic accountability and oversight?

Good practice in legal safeguards

Germany:
Obligation to immediately delete data tied to rejected applications

In case the Independent Committee rejects a bulk SIGINT application aimed at EU bodies or EU member state institutions, all data that has been acquired based on this application needs to be immediately destroyed (Section 10 (2) and (3) BND Act). The Act further includes the obligation to delete all data that may have been collected with the use of an unlawful search term.

The Netherlands:
Obligation to destroy data from bulk collection that is deemed irrelevant

The Dutch require that data from bulk collection has to be destroyed as soon as it has been determined to be irrelevant to an intelligence investigation.

127 Konkel, «The Details About the CIA's Deal With Amazon,» July 17, 2014, https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

France:
Obligation to record data deletions

Section 854-6 of the French foreign intelligence law demands that «the destruction of collected intelligence, of ‹transcriptions› and ‹extractions› are carried out by individually designated and authorized agents and must be recorded.»[128]

Canada:
Obligation to delete health data in foreign datasets

Section 11.1 (1 a) of Bill C-59 states that the services have the obligation «in respect of a Canadian dataset or a foreign dataset, to delete any information in respect of which there is a reasonable expectation of privacy that relates to the physical or mental health of an individual.»

Good practice in oversight

Sweden:
Running statistical pattern analyses on the amount of deleted material

The reviews of the Swedish oversight body, the State Inspection for Defense Intelligence Operations (SIUN), have to check how the rules concerning obligations to delete are applied. «A starting point for the review is statistical monitoring of the amount of destroyed material in order to respond to deviations.»[129]

Reviewing all deleted material is not feasible. Using statistical anomalies as leads for further in-depth controls appears to be an effective way to allocate available oversight resources. To make patterns in the destruction of data visible, audit trails of data deletion have to be available over longer time periods. Such a deviation could, for example, be an unusual peak in deletion activities at a certain point or on a certain day.

128 Article L. 854-6. of French Law No. 2015-1556 on international surveillance (own translation).
129 Swedish State Inspection for Defense Intelligence Operations (SIUN), «Årsredovisning för 2017,» February 22, 2018, Section 4.1, http://www.siun.se/dokument/Arsredovisning_2017.pdf.

Norway: Independent review of compliance with deletion obligations

The EOS Committee addressed the challenges relating to deletion in its latest annual report and demanded that the service must «shortly find a solution to prevent the processing of information when the basis for processing has ceased to exist.»[130]

Summary of main findings and reform agenda

Bulk data processing presents several complex governance challenges that will occupy oversight bodies for years to come. To put it mildly, there is plenty of room for oversight innovation. This chapter has introduced a few laudable practices that have recently been initiated in this regard. Clearly, gaps remain in many countries when it comes to issues such as the rules and procedures for data destruction and data storage for foreign intelligence.

When drafting intelligence legislation, lawmakers may not have been sufficiently mindful of the role and depth of multilateral intelligence cooperation. Services exchange raw and evaluated data in enormous quantities with their foreign partners and jointly feed various databases. Legal frameworks should account for the joint responsibility that governments have for joint databases, even if they are not hosted on their territory. Furthermore, as acknowledged by the Dutch government, there is a pressing need to ensure effective oversight over joint databases, possibly in the form of multilateral oversight.

Many oversight bodies seem to agree that much more work needs to be done to independently verify that the services honor their obligations to delete data. Drafting standards for what constitutes proper deletion would be one important step in this direction. Equally interesting, we found, were the different standards that nations use as regards the originator control principle. Here, further research is necessary. What we found thus far seems to indicate that oversight bodies can successfully be exempt from the «third-party rule» without creating negative ramifications for the security – or the degree – of the intelligence shared.

130 EOS Committee, 2018, 20.

Phase 6: Analysis

A wide range of data use is relevant for this phase. There are, of course, overlaps between data processing and data analysis. Whereas data processing refers to data registration and other formal or technical data management practices, in this phase data becomes information that is relevant for political decision-making. Different automated data analysis methods serve different purposes and are governed by their own specific rules. Bulk datasets are used both to «establish links between known subjects of interest» as well as to «search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, or to identify patterns of activity that might indicate a threat.»[131] For example, contact chaining is one common method used for target discovery: «Starting from a seed selector (perhaps obtained from HUMINT), by looking at the people whom the seed communicates with, and the people they in turn communicate with (the 2-out neighbourhood from the seed), the analyst begins a painstaking process of assembling information about a terrorist cell or network.»[132]

Automated pattern analysis and anomaly detection increasingly rely on artificial intelligence (AI) methods such as machine learning and predictive analytics. «AI is expected to be particularly useful in intelligence due to the large datasets available for analysis.»[133] The risks and benefits generally associated with AI also challenge existing oversight methods and push legislators as well as oversight practitioners to creatively engage with AI as a dual-use technology. In intelligence, AI «is intended to automate the work of human analysts who currently spend hours sifting through data for actionable information. It may free them to make more efficient and timely decisions based on the data.»[134] Conversely, malicious use of AI creates new security threats that have to be mitigated.[135]

---

131 UK Home Office, Interception of Communications. Draft Code of Practice. December 2017, 52, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668941/Draft_code_-_Interception_of_Communications.pdf.

132 Government Communications Headquarters (GCHQ), «HIMR Data Mining Research Problem Book,» September 20, 2011, 12, https://www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html.

133 Hoadley and Lucas, 2018, 13.

134 The Central Intelligence Agency (CIA) has 137 projects in development that leverage AI in some capacity, e.g.: incorporating computer vision and machine learning algorithms into intelligence collection cells that would comb through footage and automatically identify hostile activity for targeting; image recognition or labeling to predict future events such as terrorist attacks or civil unrest based on wide-ranging analysis of open source information; developing algorithms to accomplish multilingual speech recognition and translation in noisy environments; geo-locating images with no associated metadata; fusing 2-D images to create 3-D models; and tools to infer a building's function based on pattern of life analysis. See Hoadley and Lucas, 2018, 9.

135 Brundage et al., «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration,» February 2018, https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

Relevant aspects

What types of data use are permissible in a given legal framework, and are there specific rules for different forms of data use? For example, procedures for each type of use, specifying the circumstances under which that specific use is permitted.

There should also be independent oversight (internal and external) over bulk data analysis techniques, including rules and safeguards as concerns the use of AI. How is the level of privacy intrusion of specific data-analysis tools measured? And what kind of material is fed into query-focused databases?

How is the convergence of different databases/ data sources regulated? For example, may bulk communications data be matched with other stored data (such as data gathered via sensors or in hacking operations) or publicly available data? If so, does such enrichment of material happen automatically?

Good practice in legal safeguards

The Netherlands: Human-in-the-loop safeguard for automated data analysis

«The services are prohibited from promoting or taking any action against a person solely based on the results of automated data analysis. For example, if a data analysis algorithm indicates that a certain person intends to commit a terrorist attack, an intelligence service cannot act based on the outcome of this algorithm alone.»[136]

The Dutch law also clarifies what possible conduct may fall under «automated data analysis.» It includes comparing datasets with each other in an automated manner, and searching on the basis of profiles in order to find specific patterns.[137] Embedding a human in the loop does not necessarily prevent analysis failures,[138] but being obliged to present other forms of proof before taking action may help to mitigate errors and false inferences.

136 Eijkman, Eijk, and Schaik, 2018, 19.

137 Dutch Act on the Intelligence and Security Services 2017, Article 60 (2).

138 Cranor, «A Framework for Reasoning About the Human in the Loop,» 2008, http://dl.acm.org/citation.cfm?id=1387649.1387650.

The Netherlands:
Legally required specialized training for analysts

The Dutch law codifies a separation of access to data, demanding that only teams consisting of specialized personnel may access and analyze warranted datasets.[139]

Similarly, in the United Kingdom, adequate arrangements must be in place that limit the number of persons to whom certain materials can be disclosed and restrict the copying of a given dataset to the minimum number necessary.[140]

Good practice in oversight

United Kingdom:
Automated internal compliance systems for data analysis

«There are computerised systems for checking and searching for potentially non-compliant uses of GCHQ's systems and premises. For example, when an authorised person selects a particular communication for examination, this person must demonstrate that the selection is necessary and proportionate; this process is subject to internal audit.»[141]

139 Explanatory memorandum concerning the amendment to the Intelligence and Security Services Act (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten), 2016, 48f., https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten.

140 Section 150 (1) (a) and (2) United Kingdom, Investigatory Powers Act 2016.

141 European Union Agency for Fundamental Rights, 2017, 59; see also: UK Home Office, «Interception of Communications. Draft Code of Practice,» February 2017, 6.14.

France:
Ex-ante review of AI experiments and data analysis techniques

The French prime minister authorizes automated data analysis based on certain parameters after the CNCTR submitted «a non-binding opinion on both the automatic processing and the parameters. The oversight body is kept informed about every modification during the operation and has permanent, complete and direct access to this processing and the intelligence gathered.»[142]

If the services want to reauthorize the automated analysis, the renewal request provided to the prime minister should contain an assessment of the relevance of prior automated analysis and the number of targets obtained. When the French intelligence service planned to use «algorithms» to identify terrorist threats based on «connection data» in 2016, the CNCTR submitted two opinions to the prime minister concerning both the architecture of the algorithms and the meaning of the connection data.[143]

Summary of findings and reform agenda

Intelligence oversight has struggled to effectively control «black boxes» for quite some time now. The increasing importance of AI is the most recent development in this regard, with potentially far-reaching implications for how intelligence analysis is conducted. Even if AI use in surveillance is only at an experimental stage, the risk of abuse and errors may already have real-life impacts. How can one ensure that accountability exists for the errors that such algorithms might make?

Oversight has to make sure it keeps abreast of such developments, with promising practices such as the Dutch «Oversight 3.0» project or the introduction of practice warrants in New Zealand currently leading the way. Additional resources and control instruments are definitely needed for oversight bodies to ensure accountability of such AI-driven surveillance operations.

Phase 7: Review & Evaluation

Compliance with legal safeguards must be ensured through comprehensive and regular judicial oversight. Examining the effectiveness of data collection measures is equally important. Overseers need to know about this to assess the political value, the cost efficiency, and the need for the reauthorization of warrants. Identifying suitable metrics and methods for this remains a considerable challenge. For example, if data

142 European Union Agency for Fundamental Rights, 2017, 97.

143 European Union Agency for Fundamental Rights, 2017, 45; CNCTR, «Premier rapport d'activité 2015/2016,» 2016, 39f., https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf.

from a certain program or collection stream never feeds into the production of intelligence reports, does this mean that the particular data collection is superfluous and a strain on the limited resources of the intelligence community? Or, in contrast, would this be tantamount to someone cancelling a fire insurance policy simply because, thus far, his or her house has not caught fire?

Relevant aspects

The scope of the review mandate of the oversight body is a core factor. Effective review presupposes that there are no gaps in the control mandate. Control remits should be defined functionally, covering all aspects of intelligence collection, as recommended by the Council of Europe.[144]

Does the competent oversight body have the sufficient resources (staff, time, money, technical expertise) to conduct meaningful reviews? Intelligence law should also define the role for oversight in assessing the political relevance of finished intelligence operations and assign the duty to the executive branch to demonstrate the efficiency of its bulk surveillance measures, despite the ubiquitous presence of open source information.

Good practice in legal safeguards

Expanding the scope of oversight

Canada:
Holistic review of SIGINT practices across different agencies[145]

Security and intelligence services tend to pursue their investigations in close cooperation with other agencies of the national security sector (police, military, customs and border security agencies). If one oversight body were to only review the activities of one specific intelligence agency, reviews would be incomplete because they would miss the role and contributions of other agencies.[146]

Against this backdrop, the National Security and Intelligence Review Agency (NSIRA) – the new oversight body foreseen in Bill C-59 – would be an integrated body with jurisdiction over activities carried out by the Canadian Security Intelligence Service

144 Council of Europe, «Democratic and Effective Oversight of National Security Services,» May 2015, 11, https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb.

145 National Security and Intelligence Review Agency Act (NSIRA Act, in planning with Bill C-59), Section 8.

146 Parsons et al., 2017, 35.

(CSIS), the CSE, as well as national security or intelligence activities of other departments to the extent that these relate to national security or intelligence.

The new British IPCO is responsible for overseeing the use of investigatory powers, not only by intelligence agencies, but also by law enforcement, prisons, local authorities, and other government agencies. Focusing review capacities in one review body in such a way is useful because the police, for example, increasingly uses electronic methods for investigatory purposes, which are less visible and controllable for an authorizing judge than classic law enforcement methods. The increased opaqueness requires additional technical expertise to review digital surveillance measures.

In the United States, the Privacy and Civil Liberties Oversight Board (PCLOB) has jurisdiction over all counterterrorism programs operated by any federal agency, even those outside of the intelligence community (e.g., the Department of Homeland Security). Although limited to counterterrorism, this extends the oversight remit across a broader spectrum of security agencies.

Regular renewal

Sunset clauses, which are a common feature in US law, for instance, are an effective tool to trigger regular evaluations and adaptations of intelligence laws. The durations of such mandatory reauthorizations may vary.

The Netherlands:
Verification of effectiveness before renewal of authorization

An obligation to submit the necessary information in writing when applying to renew the authorization of a certain surveillance measure can be the foundation for any effectiveness assessment. For instance, the accurate tagging of information helps to identify the interception stream that was at the source of a given intelligence product.

The Dutch MIVD entertains a small «Devil's Advocate» office that provides a contrary view on (selected) intelligence reports and internal procedures.

Norway:
Criminal liability for non-compliance with oversight requests

Any acting or former Norwegian intelligence service official has a duty to answer questions and comply with all requests made by the oversight body (e.g., give evidence to the committee), regardless of the level of classification. «Willful or grossly negligent infringements» with this obligation «shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.»[147]

Good practice in oversight

Early and systematic oversight involvement

United States:
No claim to deliberative privilege vis-à-vis the PCLOB

The Privacy and Civil Liberties Oversight Board is an independent agency within the executive branch.[148] Because it works from within the executive branch, the PCLOB has full access to information, in particular to materials in a deliberative stage. The government cannot claim deliberative privilege, for example attorney-client privilege, in relation to the PCLOB. It also holds the highest level of security clearance. This unfettered access is an important precondition to challenge the arguments that the government puts forward.

The official report on Section 215[149] is an example of the PCLOB's ability to successfully question and contradict the government's reasoning and claim of the effectiveness of certain measures.

---

147 Norwegian Act relating to oversight of intelligence, surveillance and security services (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven)), February 3, 1995, Section 21, https://lovdata.no/dokument/NL/lov/1995-02-03-7; English translation available in: EOS Committee, 2018, 60, https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.

148 Although the PCLOB lacks budgetary independence, i.e., it cannot argue publicly to receive more money for its activities, the independence of the mandate stems from being able to contradict the White House and its departments and adopting a dissenting point of view.

149 PCLOB, «Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court,» January 23, 2014, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

New Zealand:
Obligatory quarterly self-reporting of incidents to the Inspector General

Since 2016, all operational compliance incidents have to be registered and reported to the Inspectors General, and not just, as was the case previously, inadvertent interceptions. Such incidents include, for example: «Interception of incorrect numbers, lines, data sets or equipment (e.g. a staff member accidentally entering an incorrect telephone number); numbers intercepted correctly but subsequently abandoned by the target and/or adopted by a non-target; organisations assisting NZSIS [New Zealand Security Intelligence Service] not being given the correct or most up to date documentation relating to the particular warrant; failure to adhere to internal policy or procedures.»[150]

International cooperation of oversight bodies

Europe:
Joint review and mutual learning sessions

Over the last couple of years, cooperation between the intelligence oversight bodies of Belgium, the Netherlands, Switzerland, Norway, and Denmark has been established.[151] The participating bodies decided to conduct «a similar review investigation in all participating countries into the international cooperation between the various intelligence services with regard to the fight against foreign terrorist fighters.»[152]

150 Office of the Inspector General of Intelligence and Security Cheryl Gwyn, «Annual Report for the Year Ended 30 June 2017,» December 1, 2017, 31f., http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf.

151 The participating bodies are (thus far): The Belgian Standing Intelligence Agencies Review Committee (Comiteri), the Dutch Intelligence and Security Services Review Committee (CTIVD), the Swiss Strategic Intelligence Service Supervision and delegations from Sweden (Commission on Security and Integrity Protection), Norway (Parliamentary Oversight Committee), and Denmark (Intelligence Oversight Board); Belgian Standing Intelligence Agencies Review Committee (Comiteri), «Rapport d'activité 2015,» September 16, 2016, 80f., http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2015.pdf.

152 Comiteri, «Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations,» 2018, 82f., http://www.comiteri.be/images/pdf/Jaarverslagen/Vast-Comit-I--Activity-Report-2016.PDF; EOS Committee, 2018, 12.

The goal is to investigate the topic from different perspectives, but based on a comparable approach. Such a focus allows for gaining a more complete picture of international intelligence cooperation efforts that would otherwise be much harder for one oversight body to investigate alone. It also allows for a more substantial dialogue on the role and reform of control instruments so as to better meet actual oversight challenges.

Five Eyes:
Five Eyes Intelligence Oversight and Review Council (FIORC)

This council was created in September 2016 and is made up of members from Australia, Canada, New Zealand, the United Kingdom, and the United States.[153] This forum is supposed to foster closer linkages within the Five Eyes review and oversight community, allow for the exchange of views on subjects of mutual interest and concern, and provide room to compare oversight methodologies and explore areas where cooperation on reviews and the sharing of results is permitted and fruitful.[154]

Oversight advisory teams

The CTIVD set up a «knowledge circle» in December 2014 that consists of subject matter experts and scientists and advises the oversight body on relevant developments. Some of these experts also consult the CTIVD regarding the selection of compliance investigations.[155] IPCO has created a technology advisory panel (TAP) of scientific

153 The participating oversight bodies are: the Office of the Inspector General of Intelligence and Security of Australia; the Office of the Communications Security Establishment Commissioner and the Security and Intelligence Review Committee of Canada; the Commissioner of Security Warrants and the Office of the Inspector General of Intelligence and Security of New Zealand; the Office of the Investigatory Powers Commissioner of the United Kingdom; and the Office of the Intelligence Community Inspector General of the United States; Office of the Inspector General National Security Agency, «Semiannual Report to Congress. 1 October 2017 to 31 March 2018,» 2018, https://www.dni.gov/files/documents/FOIA/OCT2017-MAR-2018_SAR_FINAL.PDF; and also Barker, Petrie, Dawson, Godec, Purser, and Porteous, «Oversight of Intelligence Agencies: A Comparison of the ‹Five Eyes› Nations,» 2017, 9, http://apo.org.au/system/files/123831/apo-nid123831-515251.pdf.

154 The first FIORC conference – in which representatives of review bodies from all Five Eyes countries participated – took place in Ottawa, Canada, in October 2017, see: Security Intelligence Review Committee, «SIRC Annual Report 2017–2018: Building For Tomorrow: The Future Of Security Intelligence Accountability In Canada,» 2018, http://www.sirc-csars.gc.ca/anrran/2017-2018/index-eng.html.

155 CTIVD, «Kenniskring en tegenspraak CTIVD,» September 20, 2017, https://www.ctivd.nl/over-ctivd/kenniskring--en-tegenspraak.

experts led by the statistician Bernard Silverman.[156] The Inspector General of intelligence and security of New Zealand also appointed a two-person statutory advisory panel.[157]

Summary of main findings and reform agenda

With a view to the highly integrated modern security operations involving many different agencies using similar tools, some lawmakers have rightly extended the remit of oversight bodies to agencies other than intelligence services. In so doing, these oversight bodies are becoming more visible, which, in turn, may help to attract technical expertise. Another good practice that we discussed is the increasing trend toward more regular, substantive exchanges among oversight bodies. In Europe, other countries, such as France and Germany, should consider joining existing platforms for oversight cooperation.

This chapter also discussed the need to further research the efficacy of bulk surveillance measures. Governments ought to demonstrate the continued added value of SIGINT operations at a time when their intelligence services can also resort to a trove of available open source information. However, are there better criteria and sources upon which governments› cases can be assessed?

Phase 8: Reporting

After a SIGINT collection cycle has been completed, both government and oversight bodies need to be transparent and provide adequate information about both the surveillance activities undertaken by the state and their specific oversight activities thereon. To enhance public trust, the intelligence services should proactively declassify key legal documents of public interest.[158] Such releases have, for example, allowed

156 IPCO, «A Message from the Commissioner By Sir Adrian Fulford,» May 17, 2018, https://www.ipco.org.uk/Default.aspx?mid=16.1; Investigatory Powers Commissioner's Office, Twitter Posting, December 15, 2017, https://twitter.com/IPCOffice/status/941722822405013506.

157 Inspector General of Intelligence and Security of New Zealand, «About: The Intelligence and Security Agencies,» http://www.igis.govt.nz/about/.

158 The US intelligence community, for example, has released official documentation of intelligence activities and procedures, such as declassified FISC opinions, quarterly reports, and semi-annual assessments. Many of these documents can be found at http://www.icontherecord.tumblr.com. A guide to released documents is available here: https://www.dni.gov/files/CLPT/documents/Guide_to_Posted_Documents.pdf. A searchable database of all documents is available at: https://www.intel.gov/ic-on-the-record-database.

the creation of rare public and quite comprehensive accounts of different types and patterns of compliance violations over the duration of the Section 702 program.[159]

Although full transparency of oversight activities may not be possible due to secrecy requirements, the regular reporting by oversight bodies is a crucial means for public trust and accountability. For this, it ought to be as comprehensive and timely as possible.

Relevant aspects

What rules are in place regarding mandatory, periodical public reporting on surveillance measures and its democratic control? Information on oversight methods and capacities, especially with a view to bulk surveillance, should be provided to the greatest extent possible. Reports should draw a holistic picture of all intelligence activities. What contextual material and statistical information is provided to the public? What outreach activities are pursued, and how does the oversight body communicate with public?

Good practice in legal safeguards

Options for declassification

By default, all matters discussed by the German parliamentary oversight committee (PKGr) are classified. Yet, the committee can make certain procedures public if two-thirds of the members support this step. Then, individual members of the PKGr can publish a dissenting opinion («*Sondervotum*») of the specific case at hand.[160] This provision, which explicitly allows for deviations from the norm of classification and makes particular cases or activities public, can be a useful tool for oversight. In the United States, too, Executive Order 13526 on classified national security information explicitly provides for public interest declassification, stating that, «[i]n some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified.»[161]

---

159 Robyn Green has compiled highly informative documentation that informs the public about how unintentional violations may threaten the privacy of protected communications over a longer period of time «with significant and prolonged impact.» For a summary of compliance reports under Section 702 of FISA, see: Greene, «A History of FISA Section 702 Compliance Violations,» September 28, 2017, https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.

160 Section 10 (2) German Parliamentary Control Panel Act (Parlamentarisches Kontrollgremiumgesetz), July 29, 2009.

161 U.S. Government Publishing Office, Executive Order 13526, 2009, Section 3.1(d), https://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf.

Obligation to inform about errors

The United Kingdom's IP Act introduced an obligation for IPCO to inform a person of any relevant error relating to that person when it is in the public interest for the person to be informed of the error (Section 231 (1) IP Act). This responsibility to report errors refers to specific persons, which suggests that mostly targeted surveillance practices are covered by this provision. But it would also be conceivable to inform people about errors that have occurred in bulk surveillance measures. The provision is significantly curtailed in its area of application. The IP Act also includes a provision stating that a breach of a person's rights under the Human Rights Act 1998 is not sufficient to justify the reporting of an error (Section 231 (3) IP Act). If human rights breaches are not enough to trigger reporting, then it remains to be seen what kind of errors will be reported.

Good practice in oversight

Advancing transparency on oversight methods

Norway:
Reporting on non-conformities with selectors

The EOS has recently reported to the public that «non-conformity in the service's technical information collection that resulted in the unintentional collection of information from means of communication (hereinafter referred to as selectors) that were in reality Norwegian.»[162]

Albeit without much further substantiation in the actual report, it is notable that an oversight body has publicly referred to such irregularities.

United States:
PCLOB pushing for declassification

In the PCLOB's report on Section 702,[163] the oversight body was able to obtain the declassification of a large segment of information about the program.[164]

162 EOS Committee, 2018, 43f.

163 PCLOB, 2014.

164 Federation of American Scientists, «Secrecy News 07/28/14,» July 28, 2014, https://fas.org/sgp/news/secrecy/2014/07/072814.html.

This was a new phenomenon, given that requests for declassification usually either come from above – the president – or from the public. This, though, was a case of a «lateral» request by an independent federal oversight entity.

Many oversight bodies have begun to build up significant resources for communicating with the public, for example via informative public websites and Twitter accounts. More important than this, however, are advanced transparency standards and accurate and timely oversight reports. In this regard, it is commendable that the oversight bodies of Belgium, Denmark, the Netherlands, and Norway publish their annual reports now also in English. In so doing, they provide a valuable resource for comparative work.

Institutional support for whistleblowers

United States:
Expressed commitment to whistleblower protection

In July 2018, the NSA's Inspector General declassified a version of its semi-annual report, which contains its audits and investigations from October 2017 to March 2018, to Congress. The report states: «We recognize that agencies like the NSA are simply too big, and their operations too diverse, for an OIG [Office of the Inspector General] to know what is happening throughout the organization if people do not come forward when they see something they believe is wrong, and they cannot be expected to do that if they fear retaliation for doing so. The role of whistleblowers in furthering effective oversight is particularly important at an agency like the NSA, where so much of the work must be performed outside the public eye to be effective.»[165]

At the same time the Inspector General announced the creation of a whistleblower protection page on the OIG's classified website and the establishment of a whistleblower coordinator position.[166]

165 Office of the Inspector General National Security Agency, 2018, iii.

166 Clark, «NSA Watchdog Breaks Precedent By Releasing Semi-Annual Report,» July 27, 2018, https://www.govexec.com/management/2018/07/nsa-watchdog-breaks-precedent-releasing-semi-annual-report/150105/; further information about intelligence whistleblower protection in the United States is available at https://fas.org/sgp/crs/intel/R43765.pdf.

Intelligence governance will benefit from greater public knowledge of oversight activities as well as increased insights on how surveillance is conducted. Our comparative review of national oversight systems has shown that there is room for advanced transparency reporting. This includes both more information on the use of bulk powers in actual practice and the dynamics of oversight (e.g., how different control instruments have been used). Future comparative studies on reporting standards, for example on available statistics regarding the authorization process (i.e., total number of approved and rejected applications, number of authorizations with conditions, etc.) are in order. They may illustrate how oversight bodies can regain public trust. Systematic reporting on errors in bulk surveillance should also be explored.

While effective whistleblower protections remain crucial, not least in SIGINT agencies, developing more structured accounts of both successes and failures could also support public trust in the services.

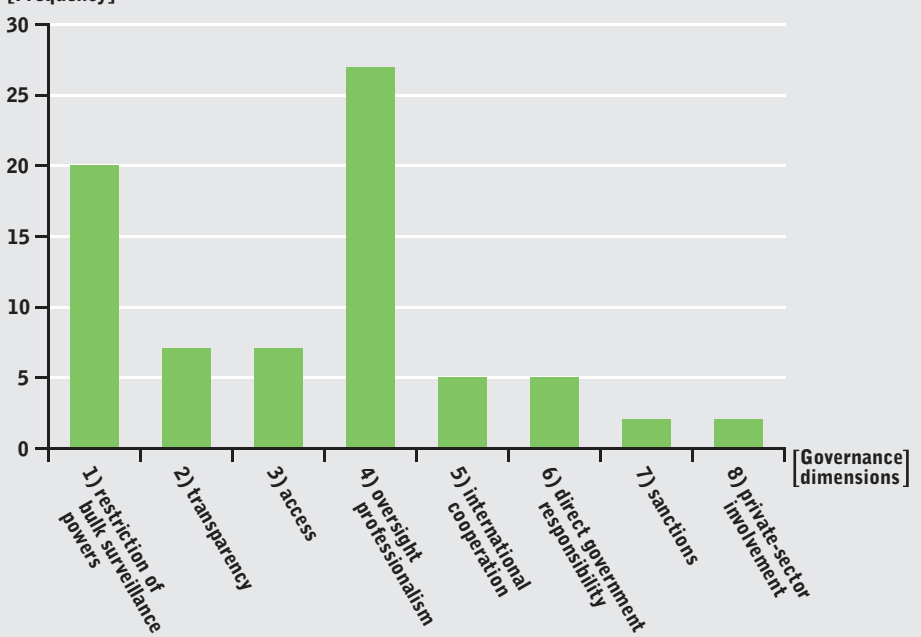
In targeted surveillance systems, persons whose private communications have been intercepted ought to be informed about this so as to provide them a chance for effective remedy. Although this may not be practicable in non-targeted foreign surveillance regimes, there might be options to introduce an obligation to inform EU citizens when their data is swept up in foreign communications data collection by a fellow European country.

IV. Discussion

Our review of legal safeguards and oversight innovations in different stages of the bulk surveillance governance process features 64 good practices. These range from ending discrimination based on citizenship to more specific authorization regimes and additional safeguards for international intelligence cooperation. Each pertains to different aspects of surveillance governance. More specifically, this includes:

- restriction of bulk surveillance powers
- transparency
- access
- oversight professionalism
- international cooperation
- direct government responsibility
- sanctions
- private-sector involvement

Figure 3: Identified dimensions of good practice



These categories are not mutually exclusive. For example, we believe that the requirement of an adequacy review of foreign cooperation partners pertains to both «international cooperation» and «oversight professionalism.» A full list of good practices and their assigned categories can be found in the Annex.

What can we learn from the dispersion of practices in the different categories? The table above shows that a majority of good practices can be tied to restrictions and the advancement of oversight professionalism. To us, this is a clear sign that lawmakers sought to overcome a lack of legitimacy in these two areas. Yet, our findings also illustrate that lawmakers tended to shy away from addressing other areas in their recent reforms – notably the direct government responsibility for the steering of surveillance measures. More concretely, we only identified five examples that pertain to this dimension. History is replete with examples in which the executive decided on the course of surveillance activities with hidden motives that may have led to malfeasances. It is important, therefore, that clear responsibilities for the important role of the executive are being established. Likewise, in the area of sanctions, which includes criminal liability for the abuse of surveillance powers, we identified only two examples. Further options to effectively sanction non-compliance on an organizational as well as individual level would strengthen the assertiveness of oversight bodies.

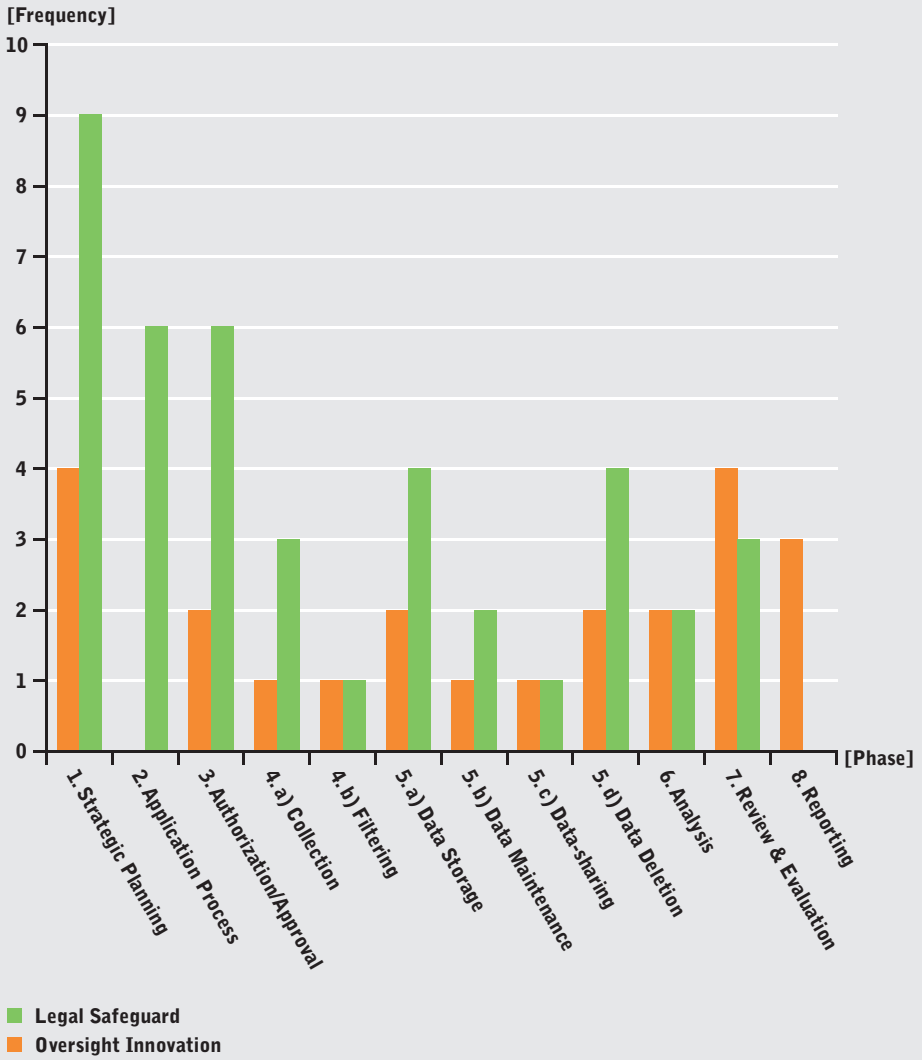
We identified seven laudable examples of advanced transparency reporting that we think merit further attention. For instance, declassifying new legal interpretations in authorization decisions is one such practice. However, here, too, there remains room for further improvements. Providing (better) statistics on the actual extent of surveillance measures (types of warrants granted, decisions on warrants and notifications, etc) and more detailed information on the auditing methods used should also figure into public reports. More transparency on the actual implementation of bulk surveillance measures will increase public trust.

Interestingly, very few reforms included rules that clearly define who is in charge of extracting the data and how providers can challenge government requests for access to data. Without private-sector involvement, most bulk collection activities would not be feasible. Provider intermediation can be an important safeguard against executive overreach, and therefore more systematic oversight-carrier dialogues should be established.

Looking at the distribution of good practice examples across the eight functional phases of our SIGINT governance analysis scheme (see figure 4), we can denote a general preference by lawmakers for legal safeguards as opposed to oversight innovation. Presumably, one reason for this could be that changes of actual oversight dynamics are labor-intensive and take time to implement. But they are equally important. Even the best laws can only go so far. Surveillance governance in democratic societies also requires the effective use of control instruments. It is in this area that oversight bodies need to work harder to keep up with technological change. Parliaments across the world are well-advised to invest not just in the latest surveillance technology but also in auditing tools for modern oversight bodies.

New tools such as technical interfaces for direct database access are major innovations in oversight practices. Unhindered and complete access to all relevant

Figure 4: Identified good practices per phase



intelligence information is extremely important for effective oversight. In this regard, though, most reform efforts remain underwhelming, especially in the area of intelligence cooperation. As multilateral cooperation among intelligence and security agencies is fast evolving, national oversight bodies need to catch up. Some oversight bodies have already begun to address this enormous task. In so doing, they will not only benefit from mutual learning. In the future, they may also find creative solutions to fix some of the current accountability deficits that international intelligence cooperation entails. As currently proposed by the Dutch CTIVD, one might also want to

start thinking creatively about the institutional design of multilateral oversight on the CTG database.

Some intelligence oversight bodies have now developed an independent voice that pushes back more often against regulatory capture and reaffirms their independence. Some have become increasingly mindful of the numerous risks that ever closer intelligence cooperation entails. They are now more influential than before due to public awareness and regulatory reform, and they tend to be better equipped to fulfill their critical democratic mission in the «golden age of surveillance.»

V. Conclusion

Reforms of bulk surveillance post-Snowden have been limited and underwhelming in the eyes of many observers. Yet, the debate about rights-based and democratically controlled surveillance governance is far from over. Although courts such as the European Court of Human Rights tend to grant a broad leeway to national governments to implement bulk surveillance, they also insist on adequate safeguards. What this means in practice, though, will not be decided by the courts. Rather, it involves the hard work of taking the lessons about ineffective oversight and applying better practices through the slow and steady channels of democratic institutions. This may not be the Snowden legacy that some expected. Yet, it is the difficult and necessary work of democratic governance.

We hope that this compendium can contribute to this effort, and we welcome feedback and any additional ideas on the good practices we selected. There are individual aspects in each intelligence reform that stand out by comparative review and merit further discussion. While better intelligence governance does not simply equal the sum of all best practices, we believe that adopting the presented legal safeguards and oversight practices in other countries will raise the bar for democratic standards in intelligence governance.

Good oversight is also good security. Citizens rightfully expect accountable, necessary, and effective modes of governing intelligence in the digital age. This must include legal safeguards and oversight practice, as both aspects play a crucial role in providing security for all. This is because effective oversight, in contrast, pushes governments to be as effective as possible in allocating their resources and selecting their targets. Implementing clear intelligence priorities (phase 1) and specific and robust authorizing mechanisms (phases 2 and 3 of our scheme) are key to accomplish that. Similarly, the collection, processing, and analysis (phases 4, 5 and 6, respectively) of communications are equally significant stages of the intelligence process. There are many potential forms of abuse that can be tied to these moments, which is why both intelligence legislation and oversight practice need to apply beyond the initial authorization moment. Moreover, with a view to institutional learning and public confidence in intelligence governance, the professional review and enhanced public reporting on modern bulk surveillance activities (phases 7 and 8) are fundamentally important. In the Appendix, we list 64 promising examples from all eight phases of the bulk surveillance process.

Naturally, the quest for better democratic control and governance of bulk surveillance is ongoing. Authorization bodies, courts, parliamentary committees, internal compliance departments, executive control and independent review agencies all play a vital role in maintaining and promoting public trust in intelligence activities. But the

burden to provide sufficient transparency and to demonstrate legal compliance rests also with the intelligence services themselves. As some examples in this compendium have shown, they can work harder in some countries than in others to release sufficient information for public scrutiny.

We hope that by presenting laudable aspects in either national intelligence laws or reformed oversight practices, we have contributed to the necessary debate on how to trim and effectively oversee bulk surveillance powers. Positive change, though, may not come from the identification of good practices alone. They need to be debated and become part of a broader national reform agenda. Yet, lawmakers who are now seriously discussing these practices with civil society organizations and the executive may eventually decide to adopt some of these good practices. We stand ready to offer our advice and encourage them to collectively up the ante for the protection and promotion of our security and our privacy.

VI. Annex

List of Workshop Participants

Many people offered their advice and expert knowledge to us. We received constructive feedback and additional information in a series of interviews and during two expert workshops in Berlin.

We are very grateful for the help we received and for the interest and time that a wide range of different stakeholders have invested in our project. The views and opinions expressed in this document are our own.

The following experts provided valuable input on earlier versions of this report during a workshop on June 14 and 15, 2018, in Berlin.

- Sharon Bradford Franklin, Director of Surveillance and Cybersecurity Policy, New America's Open Technology Institute
- Iain Cameron, Professor at Department of Law, Uppsala University and Swedish Member of the Venice Commission, Council of Europe
- Joan Feigenbaum, Grace Murray Hopper Professor of Computer Science, Yale University
- Giles Herdale, Policy Advisor and Co-chair, Independent Digital Ethics Panel for Policing
- Eric King, Visiting Lecturer at Queen Mary University of London
- Ronja Kniep, Research Fellow, Berlin Social Science Center (WZB)
- Klaus Landefeld, Director Infrastructure & Networks at eco – Association of the Internet Industry and Supervisory Board member of DE-CIX International
- Greg Nojeim, Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy & Technology
- Jörg Pohle, PostDoc, Alexander von Humboldt Institute for Internet and Society (HIIG)
- Volker Roth, Professor of Computer Science, Freie Universität Berlin
- Graham Smith, Partner, Bird & Bird LLP
- Eric Töpfer, Senior Researcher, German Institute for Human Rights
- Nico van Eijk, Professor of Media and Telecommunications Law and Director of IViR, University of Amsterdam
- Njord Wegge, Senior Research Fellow, Norwegian Institute of International Affairs (NUPI)

The following oversight officials provided valuable input on an earlier version of this report during a workshop on May 14, 2018, in Berlin. Not all participants agreed to be named, hence this is not a comprehensive list of all workshop participants.

- Frank Brasz, Deputy General Secretary, CTIVD, the Netherlands
- Wouter de Ridder, Standing Intelligence Agencies Review Committee, Belgium
- Arild Færaas, EOS Committee's secretariat, Norway
- Emil Bock Greve, Intelligence Oversight Board, Denmark
- Bertold Huber, Deputy Chair, G10-Kommission, Germany
- Rune Odgaard Jensen, Intelligence Oversight Board, Denmark
- Jantine Kervel-de Goei, General Secretary, CTIVD, the Netherlands
- Charles Miller, Investigatory Powers Commissioner's Office, United Kingdom
- Dominic Volken, Deputy Head, Independent Oversight Authority for Intelligence Activities, Switzerland

List of Interviewed Experts

Not all interviewees agreed to be named. Please note, therefore, that this is not a comprehensive list of all interviews conducted.

- Marie-Laure Basilien-Gainche, Professor of Law, University Jean Moulin Lyon 3, Honorary member of the Institut Universitaire de France
- Susan Decker, Senior Research Advisor, Legal Counsel, Security Intelligence Review Committee, Canada
- Craig Forcese, Professor of Law, University of Ottawa
- Lex Gill, Research Fellow, Citizen Lab, University of Toronto
- Elspeth Guild, Professor of Law, Queen Mary University of London
- Lotte Houwing, File Coordinator, Public Interest Litigation Project
- Peter Koop, Electrospaces.net
- Sébastien-Yves Laurent, Professor at the University of Bordeaux – Faculty of Law and Political Science
- Evan Light, Assistant Professor, Communications Program, Glendon College, York University
- Simon McKay, Barrister in Civil Liberties and Human Rights Law
- Brenda McPhail, Director, Privacy, Technology & Surveillance Project, Canadian Civil Liberties Association
- David Medine, Former chair of the US Privacy and Civil Liberties Oversight Board
- Mario Oetheimer, Head of Sector Information Society, Privacy and Data Protection, Freedoms and Justice Department, European Union Agency for Fundamental Rights
- Jonathan Obar, Assistant Professor, Department of Communication Studies, York University
- Félix Tréguer, Post-Doc Researcher, Sciences Po Paris

List of Good Practices

#	Example Practice	Phase	Dimension	Country*	Category
1	No discrimination between foreign and domestic data in intelligence collection	Strategic Planning	Legal Safeguard	NL	Restriction 
2	Restricting the use of bulk powers: PPD 28 prioritizes targeted collection over bulk	Strategic Planning	Legal Safeguard	USA	Restriction 
3	Transparency on actors involved in formulating the National Intelligence Priority Framework	Strategic Planning	Legal Safeguard	D	Transparency 
4	Annual review of any intelligence priorities by heads of departments	Strategic Planning	Legal Safeguard	USA	Government responsibility 
5	Adequacy Review of Foreign Cooperation Partners	Strategic Planning	Legal Safeguard	NL	International cooperation  Professionalism 
6	Written agreements on the aims, the nature, and the duration of international cooperation must be approved by Chancellery	Strategic Planning	Legal Safeguard	D	International cooperation  Government responsibility 
7	Prohibition of economic espionage	Strategic Planning	Legal Safeguard	D	Restriction 

#	Example Practice	Phase	Dimension	Country*	Category
8	Prohibition of discrimination against protected classes through bulk collection	Strategic Planning	Legal Safeguard	USA	Restriction 
9	Criminal liability for willful real-time surveillance conducted for an unlawful purpose	Strategic Planning	Legal Safeguard	USA	Sanction 
10	Parliamentary committee must be informed regularly about operational purposes	Strategic Planning	Oversight	UK	Transparency 
11	Full access to documentation of cooperation agreements	Strategic Planning	Oversight	CA	International cooperation  Access 
12	CTIVD can review the weighting notes	Strategic Planning	Oversight	NL	International cooperation  Access 
13	Parliamentary oversight committee must be informed about all MoU	Strategic Planning	Oversight	D	International cooperation  Access 
14	Restriction on the number of agencies allowed to use the data	Warrantry	Legal Safeguards	F	Restriction 

#	Example Practice	Phase	Dimension	Country*	Category
15	Type of automated processing accounted for in warrants	Warrantry	Legal Safeguards	F	Professionalism 
16	Specific requirements to make the «intelligence case» in a bulk SIGINT application	Warrantry	Legal Safeguards	CA	Restriction  Professionalism 
17	Listing of search terms in untargeted communications data surveillance warrants	Warrantry	Legal Safeguards	D	Restriction  Professionalism 
18	Predefining specific fiber optic cables to be intercepted	Warrantry	Legal Safeguards	NL	Restriction 
19	Direct ministerial responsibility for the activation of certain search terms	Warrantry	Legal Safeguards	D	Government responsibility 
20	Option to approve a warrant with conditions	Authorization/ Approval	Legal Safeguards	CA	Professionalism 
21	Mandatory public report by authorization body	Authorization/ Approval	Legal Safeguards	NL	Transparency 
22	Option to request publication of a Foreign Intelligence Surveillance Court decision or opinion	Authorization/ Approval	Legal Safeguards	USA	Transparency 
23	Required declassification review for new legal interpretations	Authorization/ Approval	Legal Safeguards	USA	Transparency 

#	Example Practice	Phase	Dimension	Country*	Category
24	Option to request external legal opinion in authorization procedures	Authorization/ Approval	Legal Safeguards	USA	Professionalism 
25	Quotas for specific data collection methods	Authorization/ Approval	Legal Safeguards	F	Restriction 
26	IPCO Advisory Notice	Authorization/ Approval	Oversight	UK	Professionalism 
27	Open oversight – civil society dialogue on proportionality standards for the review of bulk powers	Authorization/ Approval	Oversight	UK	Professionalism 
28	Specialized executive body serves as data collection center	Collection	Legal Safeguards	F	Government responsibility 
29	Options for providers to object to government requests for data	Collection	Legal Safeguards	USA	Private sector involvement 
30	ISPs responsible for installing splitters and selector lists	Collection	Legal Safeguards	USA	Private sector involvement 
31	Installation of interfaces	Collection	Oversight	F NL NOR CH	Professionalism 
32	All raw data (including content and metadata) that gets filtered out will be impossible to retrieve by the intelligence services	Filtering	Legal Safeguards	NL	Restriction 

#	Example Practice	Phase	Dimension	Country*	Category
33	The FISC reviews compliance audits performed by the intelligence community	Filtering	Oversight	USA	Access 
34	No distinction between metadata and content	Data Storage	Legal Safeguards	NL	Restriction 
35	Obligation to keep a file classification scheme	Data Storage	Legal Safeguards	D	Professionalism 
36	Appropriations clause for joint databases	Data Storage	Legal Safeguards	D	Professionalism 
37	Equalized SIGINT retention rules for US persons and non-US persons	Data Storage	Legal Safeguards	USA	Restriction 
38	Oversight 3.0 project on future challenges run by oversight body	Data Storage	Oversight	NL	Professionalism 
39	Joint inspections of judicial oversight body and DPA	Data Storage	Oversight	D	Professionalism 
40	Duty of care and relevance as regards data processing, including the use of algorithms	Data Maintenance	Legal Safeguards	NL	Government responsibility 
41	Mandatory tagging of all bulk SIGINT data	Data Maintenance	Legal Safeguards	D	Restriction  Professionalism 

#	Example Practice	Phase	Dimension	Country*	Category
42	Mandatory ex-ante opinion by oversight body on the data-tagging process	Data Maintenance	Oversight	F	Restriction  Professionalism 
43	By default full access to all information for oversight body	Data-sharing	Legal Safeguards	NOR	Access 
44	Random sample checks on automatic transfers of personal data to foreign intelligence services	Data-sharing	Oversight	D	Professionalism 
45	Obligation to immediately delete data tied to rejected applications	Data Deletion	Legal Safeguard	D	Restriction 
46	Obligation to destroy data from bulk collection that is deemed irrelevant	Data Deletion	Legal Safeguard	NL	Restriction 
47	Obligation to record data deletions	Data Deletion	Legal Safeguard	F	Professionalism  Restriction 
48	Obligation to delete health data in foreign datasets	Data Deletion	Legal Safeguard	CA	Restriction 
49	Running statistical pattern analyses on the amount of deleted material	Data Deletion	Oversight	SWE	Professionalism 
50	Independent review of compliance with deletion obligations	Data Deletion	Oversight	NOR	Professionalism 

#	Example Practice	Phase	Dimension	Country*	Category
51	Human-in-the-loop safeguard for automated data analysis	Analysis	Legal Safeguards	NL	Professionalism 
52	Legally required specialized training for analysts	Analysis	Legal Safeguards	NL	Professionalism 
53	Automated internal compliance systems for data analysis	Analysis	Oversight	UK	Professionalism  Restriction 
54	Ex-ante review of AI experiments and data analysis techniques	Analysis	Oversight	F	Professionalism 
55	Holistic review of SIGINT practices across different agencies	Review & Evaluation	Legal Safeguards	CA	Access  Professionalism 
56	Verification of effectiveness before renewal of authorization	Review & Evaluation	Legal Safeguards	NL	Restriction 
57	Criminal liability for non-compliance with oversight requests	Review & Evaluation	Legal Safeguards	NOR	Sanction 
58	No claim to deliberative privilege vis-à-vis the PCLOB	Review & Evaluation	Oversight	USA	Access 
59	Obligatory quarterly self-reporting of incidents to the Inspector General	Review & Evaluation	Oversight	NZ	Professionalism 

#	Example Practice	Phase	Dimension	Country*	Category
60	Joint review and mutual learning sessions	Review & Evaluation	Oversight	BE NL CH NOR DK	Professionalism 
61	Five Eyes Intelligence Oversight and Review Council	Review & Evaluation	Oversight	AUS CA NZ UK USA	Professionalism 
62	Reporting on non-conformities with selectors	Reporting	Oversight	NOR	Transparency 
63	PCLOB pushing for declassification	Reporting	Oversight	USA	Transparency 
64	Expressed commitment to whistleblower protection	Reporting	Oversight	USA	Transparency 

* BE = Belgium; CA = Canada; CH = Switzerland; D = Germany; DK = Denmark; F = France; NL = the Netherlands; NOR = Norway; NZ = New Zealand; SWE = Sweden; UK = United Kingdom; USA = United States

List of Abbreviations

Abbreviation	Name	English translation
AB-ND	Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten	Independent supervisory authority on intelligence activities (Switzerland)
AI	Artificial Intelligence	
AIVD	Algemene Inlichtingen en Veiligheids-dienst	General Intelligence and Security Service (the Netherlands)
BND	Bundesnachrichtendienst	Federal Intelligence Service (Germany)
BND Act	Gesetz über den Bundesnachrichten-dienst	Act on the Federal Intelligence Service (Germany)
BVerfG	Bundesverfassungsgericht	The Federal Constitutional Court (Germany)
BVerfSch Act	Bundesverfassungsschutzgesetz	Act on the Federal Office for the Protection of the Constitution (Germany)
CJEU	Court of Justice of the European Union	
CNCTR	Commission nationale de contrôle des techniques de renseignement	National Commission of Control of the Intelligence Techniques (France)
COMINT	Communication Intelligence	
CSE	Communications Security Establishment (Canada)	
CSIS	Canadian Security Intelligence Service	
CTG	Counter Terrorism Group	
CTIVD	De Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten	Oversight Committee for the Intelligence and Security Services (the Netherlands)
DNI	Director of National intelligence (USA)	
DPA	Data Protection Authority	
ECtHR	European Court of Human Rights	
EOS	Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste	Parliamentary Intelligence Oversight Committee (Norway)
FIORC	Five Eyes Intelligence Oversight and Review Council	
FISA	Foreign Intelligence Surveillance Act (USA)	

Abbreviation	Name	English translation
FISC	United States Foreign Intelligence Surveillance Court (USA)	
G10 Act	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz)	Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (Germany)
G10 Commission	G10-Kommission	Quasi-judicial authorization body of the German federal parliament (Germany)
GCHQ	Government Communications Headquarters (UK)	
GIC	Groupement interministériel de contrôle	Inter-ministerial control group under the purview of the prime minister (France)
HUMINT	Human Intelligence	
ISP	Internet Service Provider	
IP Act	Investigatory Power Act (UK)	
IPCO	Investigatory Powers Commissioner's Office (UK)	
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	Military Intelligence and Security Service (The Netherlands)
MoU	Memorandum of Understanding	
ND Act	Nachrichtendienstgesetz	Federal Intelligence Service Act (Switzerland)
NDB	Nachrichtendienst des Bundes	Federal Intelligence Service (Switzerland)
NSA	National Security Agency (USA)	
NSIRA	National Security and Intelligence Review Agency (Canada)	
NZSIS	New Zealand Security Intelligence Service	
PCLOB	The Privacy and Civil Liberties Oversight Board (USA)	
PKGr	Parlamentarisches Kontrollgremium	Parliamentary Control Panel (Germany)
PPD 28	Presidential Policy Directive 28 on Signals Intelligence Activities (USA)	

Abbreviation	Name	English translation
SIGINT	Signals Intelligence	
SIUN	Statens inspektion för försvarsunder-rättelseverksamheten	The State Inspection for Defense Intelligence Operations (Sweden)
TAP	Technology Advisory Panel (UK)	
TIB	Toetsingscommissie Inzet Bevoegdheden	Review Board for the Use of Powers (The Netherlands)

Bibliography

Administrative Office of the United States Courts. 2018. «Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017.» April 25, 2018. http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.

Anderson, David. 2015. «A Question of Trust: Report of the Investigatory Powers Review.» London: Independent Reviewer. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

——. 2016. «Report of the Bulk Powers Review,» London: Independent Reviewer. https://terrorism-legislationreviewer.independent.gov.uk/bulk-powers-review-report/.

——. 2018. «New Approaches to Intelligence Oversight in the U.K.» *Lawfare*. January 2, 2018. https://www.lawfareblog.com/new-approaches-intelligence-oversight-uk.

Barker, Cat, Claire Petrie, Joanna Dawson, Samantha Godec, Pleasance Purser, and Holly Porteous. 2017. «Oversight of Intelligence Agencies: A Comparison of the ‹Five Eyes› Nations.» Parliamentary Library, Research Paper Series 2017–18. Parliament of Australia. Department of Parliamentary Services. http://apo.org.au/system/files/123831/apo-nid123831-515251.pdf.

Belgian Standing Intelligence Agencies Review Committee (Comiteri). 2016. «Rapport d'activité 2015.» http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2015.pdf.

——. 2018. «Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations.» Brussels. http://www.comiteri.be/images/pdf/Jaarverslagen/Vast-Comit-I--Activity-Report-2016.PDF.

Bellovin, Steven M., Matt Blaze, Susan Landau, and Stephanie K. Pell. 2016. «It's Too Complicated: How the Internet Upends Katz, F, and Electronic Surveillance Law.» *Harvard Journal of Law & Technology* 30 (1). https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf.

Bos-Ollermann, Hilde. 2017. «Mass Surveillance and Oversight.» In *Surveillance, Privacy and Trans-Atlantic Relations*, edited by David D. Cole, Federico Fabbrini, and Stephen J. Schulhofer. *Hart Studies in Security and Justice*, Volume 1. Oxford: Hart Publishing.

Bradford Franklin, Sharon. 2018. «Carpenter and the End of Bulk Surveillance of Americans.» *Lawfare*. July 25, 2018. https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, et al. 2018. «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration.» February 2018. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

Carey, Bjorn. 2016. «Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information». Stanford News (blog), 16 May 2016. https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/.

Chopin, Olivier. 2017. «Intelligence Reform and the Transformation of the State: The End of a French Exception.» *Journal of Strategic Studies* 40 (4): 532–53. https://doi.org/10.1080/01402390.2017.1326100.

Clark, Charles S. 2018. «NSA Watchdog Breaks Precedent By Releasing Semi-Annual Report.» *Government Executive*. July 27, 2018. https://www.govexec.com/management/2018/07/nsa-watchdog-breaks-precedent-releasing-semi-annual-report/150105/.

Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten (CTIVD). 2015. «Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX.» August 26, 2015. https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel.

——. 2016. «Review Report on the Implementation of Cooperation Criteria by the AIVD and the MIVD.» CTIVD no. 48. https://english.ctivd.nl/documents/review-reports/2016/12/22/index48.

——. 2017. «Kenniskring en tegenspraak CTIVD – Over CTIVD.» September 20, 2017. https://www.ctivd.nl/over-ctivd/kenniskring--en-tegenspraak.

——. 2018. «Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD.» CTIVD No. 56. https://english.ctivd.nl/documents/review-reports/2018/04/24/index.

Commission nationale de contrôle des techniques de renseignement (CNCTR). 2016. «Premier rapport d'activité 2015/2016.» https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf.

——. 2018. «Deuxième Rapport d'activité 2017.» https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf.

Conger, Kate. 2017. «An Unknown Tech Company Tried (and Failed) to Stop the NSA's Warrantless Spying.» *Gizmodo*. June 14, 2017. https://gizmodo.com/an-unknown-tech-company-tried-and-failed-to-stop-the-1796111752.

Cook, Ben. 2017. «The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty.» *American University Law Review* 66 (2, Article 5). http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1960&context=aulr.

Council of Europe. 2015. «Democratic and Effective Oversight of National Security Services.» Strasbourg. https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb.

Court of Justice of the European Union. 2016. «C-203/15 Tele2 Sverige AB v Post-Och Telestyrelsen and C-698/15 SSHD v Tom Watson & Others.» December 16, 2016. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=186492&occ=first&dir=&cid=406338.

Cranor, Lorrie Faith. 2008. «A Framework for Reasoning About the Human in the Loop.» In *Proceedings of the 1st Conference on Usability, Psychology, and Security*. UPSEC'08. Berkeley, CA: USENIX Association. http://dl.acm.org/citation.cfm?id=1387649.1387650.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). 2016. «Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041).» Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. https://www.bundestag.de/blob/459634/a09df397dff6584a83a43a334f3936a3/18-4-660-data.pdf.

——. 2017. «26. Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016.» Bonn. https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=3.

Donohue, Laura K. 2017. «The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law.» https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law.

Dorion, Pierre. 2008. «Data Deletion or Data Destruction?» *SearchDataBackup*. July 2008. https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction.

Dreo Rodosek, Gabi. 2016. «Sachverständigengutachten. Beweisbeschluss SV-13, 1. Untersuchungsausschuss der 18. Wahlperiode,» September 30, 2016, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisation_rodosek.pdf.

German Federal Constitutional Court (BVerfG). 2005. «Leitsätze Zum Urteil Des Zweiten Senats Vom 12. April 2005 (2 BvR 581/01).» https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2005/04/rs20050412_2bvr058101.pdf;jsessionid=969575C316AC611F8F71AAB2F6C75D6F.1_cid394?__blob=publicationFile&v=1.

Eijk, Nico van, and Cedric Ryngaert. 2017. «Expert Opinion – Legal Basis for Multilateral Exchange of Information.» Appendix IV bij CTIVD rapport no. 56 to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD. Utrecht/Amsterdam. https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv.

Eijkman, Quirine, Nico van Eijk, and Robert van Schaik. 2018. «Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?» Institute for Information Law (IViR, University of Amsterdam). https://www.ivir.nl/publicaties/download/Wiv_2017.pdf.

Electronic Frontier Foundation. 2013. «Yahoo's Challenge to the Protect America Act in the Foreign Intelligence Court of Review.» October 22, 2013. https://www.eff.org/cases/yahoos-challenge-protect-america-act-foreign-intelligence-court-review.

Electrospaces.net. 2018. «Collection of Domestic Phone Records under the USA Freedom Act.» July 14, 2018, https://electrospaces.blogspot.com/2018/07/collection-of-domestic-phone-records.html

European Court of Human Rights. 2010. «Case of Kennedy v. The United Kingdom (Application No. 26839/05).» Strasbourg.

——. 2015. «Case of Roman Zakharov v. Russia (Application No. 47143/06).» Judgment. Strasbourg. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}.

——. 2016. «Case of Szabó and Vissy v. Hungary (Application No. 37138/14).» January 12, 2016. Strasbourg. http://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf.

——. 2018a. «Case of Paul Popescu v. Romania (Application No. 64162/10).» Strasbourg. https://www.juridice.ro/wp-content/uploads/2018/02/CASE-OF-PAUL-POPESCU-v.-ROMANIA.pdf.

——. 2018b. «Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08).» Strasbourg. http://www.statewatch.org/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf.

European Court of Human Rights, and Council of Europe. 1978. «Case of Klass and Others v. Germany (Application No. 5029/71).» Strasbourg. September 6, 1978. https://stewartroom.co.uk/wp-content/uploads/2014/07/Cases-ECHR-Klass.pdf.

——. 2009. «Case of Iordachi and Others v. Moldova (Application No. 25198/02).» Strasbourg. https://rm.coe.int/168067d212.

European Union Agency for Fundamental Rights. 2015. «Surveillance by Intelligence Services – Volume I: Member States› Legal Frameworks.» October 22, 2015. http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

——. 2017. «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update.» October 18, 2017. http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega.

Farrell, Henry. 2016. «America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?» *Washington Post*. June 14, 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/.

Federation of American Scientists, «Secrecy News 07/28/14,» July 28, 2014, https://fas.org/sgp/news/secrecy/2014/07/072814.html..

Forcese, Craig. 2018. «Bill C-59 and the Judicialization of Intelligence Collection. Draft Working Paper 04-06-18.» *Ottawa Faculty of Law Working Paper No. 2018-13.*, 13.

Führungsunterstützungsbasis FUB. n.d. «Die Organisation Der FUB – ZEO (Elektronische Operationen).» https://www.vtg.admin.ch/de/organisation/fub.html.

Gallagher, Ryan. 2016. «Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure.» *The Intercept*. June 7, 2016. https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/.

Goldman, Zachary K., and Samuel J. Rascoff (eds.). 2016. *Global Intelligence Oversight. Governing Security in the Twenty-First Century*. Oxford: Oxford University Press.

Government Communications Headquarters (GCHQ). 2011. «HIMR Data Mining Research Problem Book.» September 20, 2011. https://www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html.

Government of France. n.d. «Groupement Interministériel de Contrôle (GIC).» *Gouvernement.fr*. https://www.gouvernement.fr/groupement-interministeriel-de-controle-gic.

Graulich, Kurt. 2017. «Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und Internationale Datenkooperation.» *Kriminalpolitische Zeitschrift* 1: 43–52.

Greene, Robin. 2017. «A History of FISA Section 702 Compliance Violations.» *New America*. September 28, 2017. https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.

Hoadley, Daniel S., and Nathan J. Lucas. 2018. «Artificial Intelligence and National Security.» Congressional Research Service. April 26, 2018. https://fas.org/sgp/crs/natsec/R45178.pdf.

Houwing, Lotte. 2018. «The Wiv 2017. A Critical Contemplation of the Act in an International Context.» https://www.burojansen.nl/pdf/2018-LotteHouwing-WivCriticalContemplation_final.pdf.

Huber, Bertold. 2017. «Kontrolle der Nachrichtendienste des Bundes – Dargestellt am Beispiel der Tätigkeit der G10-Kommission.» *Zeitschrift für das Gesamte Sicherheitsrecht*, no. 01. https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5CGSZ%5C2017%5Ccont%5CGSZ.2017.H01.gl2.htm.

Human Rights Watch. 2017. «Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act.» *Human Rights Watch*. September 14, 2017. https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance.

Inspector General of Intelligence and Security of New Zealand. n.d. «About: The Intelligence and Security Agencies.» http://www.igis.govt.nz/about/.

International Network of Civil Liberties Organizations. 2018. «Unanswered Questions – International Intelligence Sharing.» June. https://www.inclo.net/pdf/iisp/unanswered_questions.pdf.

Investigatory Powers Commissioner's Office. 2018a. «IPCO Advisory Notice: Approval of Warrants, Authorisations and Notices by Judicial Commissioners.» 01/2018. London. https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf.

——. 2018b. «A Message from the Commissioner by Sir Adrian Fulford.» *IPCO Blog*. May 17, 2018. https://www.ipco.org.uk/Default.aspx?mid=16.1.

——. 2018c. «IPC Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers,» May 23, 2018. https://www.ipco.org.uk/docs/IPC_Submissions_on_bulk_powers.pdf.

Konkel, Frank. 2014. «The Details About the CIA's Deal with Amazon.» *The Atlantic*, July 17, 2014, https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

Kris, David S., and J. Douglas Wilson. 2012. *National Security Investigations & Prosecutions 2d*. National Security Investigations & Prosecutions 2d 1. West. https://books.google.de/books?id=THYfMwEACAAJ.

Laperruque, Jake. 2018. «After ‹Foreign Surveillance› Law, Congress Must Demand Answers from Intelligence Community.» *The Hill*, January 2018. https://thehill.com/opinion/cybersecurity/370271-after-foreign-surveillance-law-congress-must-demand-answers-from.

«Le Groupement interministériel de contrôle va beaucoup donner.» 2016. *Defense – La voix du nord*. February 1, 2016. http://defense.blogs.lavoixdunord.fr/archive/2016/02/01/groupement-interministeriel-de-controle-14495.html.

Leigh, Ian, and Njord Wegge (eds.). 2018. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. 1 edition. Routledge.

Lubin, Asaf. 2017. «‹We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance.» SSRN Scholarly Paper ID 3008428. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3008428.

——. 2018. «Legitimizing Foreign Mass Surveillance in the European Court of Human Rights.» *Just Security*. August 2, 2018. https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

Malgieri, Gianclaudio, and Paul De Hert. 2017. «European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‹Good Enough› Oversight, Preferably but Not Necessarily by Judges.» In *Cambridge Handbook of Surveillance Law, Forthcoming 2017*, edited by D. Gray and S. Henderson. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2948270.

McKay, Simon. 2018. *Blackstone's Guide to the Investigatory Powers Act 2016*. Oxford, New York, NY: Oxford University Press.

McKay, Simon, and Clive Walker. 2017. «Legal Regulation of Intelligence Services in the United Kingdom.» In *Handbuch des Rechts der Nachrichtendienste*. Stuttgart: Richard Boorberg.

Menn, Joseph. 2016. «Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources.» *Reuters*, October 5, 2016. https://www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2016. «Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten.» Kamerstuk. October 28, 2016. https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten.

——. 2017. «Bijlage bij brief Wiv 2017 en regeerakkoord,» 2017. https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2017/12/15/kamerbrief-over-wiv-2017-en-het-regeerakkoord/20171215+Bijlage+bij+brief+minister+BZK+over+Wiv+2017+en+regeerakkoord.pdf.

Murray, Daragh, Pete Fussey, and Maurice Sunkin. 2018. «Response to Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers.» https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf.

National Security Agency/ Central Intelligence Agency. 2012. «(U)SIGINT Strategy 2012-2016.» February 23, 2012. https://edwardsnowden.com/wp-content/uploads/2013/11/2012-2016-sigint-strategy-23-feb-12.pdf.

Necessary and Proportionate Coalition. 2014. «Necessary & Proportionate. International Principles on the Application of Human Rights to Communications Surveillance.» May 2014. https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.

Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee). 2016. «Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget).» February 29, 2016. Oslo. https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf.

——. «Annual Report 2017 – Document 7:1 (2017–2018).» Oslo. https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.

Nyst, Carly. 2018. «Regulation of Big Data Surveillance by Police and Intelligence Agencies.» The Human Rights, Big Data and Technology Project, University of Essex. https://1ing2s14id7e20wtc8xsceyr-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Regulation-of-Big-Data-Surveillance-by-Police-and-Intelligence-Agencies.pdf.

Office of the Inspector General National Security Agency. 2018. «Semiannual Report to Congress. 1 October 2017 to 31 March 2018.» https://www.oversight.gov/report/nsa/semi-annual-report-congress-1-october-2017-31-march-2018.

Office of the Inspector General of Intelligence and Security Cheryl Gwyn. 2017. «Annual Report for the Year Ended 30 June 2017.» December 1, 2017. Wellington. http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf.

Ohm, Paul. 2010. «The Argument against Technology-Neutral Surveillance Laws,» no. 88 Tex. L. Rev. 1685. https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=.

Organisation for Economic Co-Operation and Development. 2013. «The OECD Privacy Framework.» https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert. 2017. «Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters), First Reading (December 18, 2017).» The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf.

Perry, Rodney M. 2014. «Intelligence Whistleblower Protections: In Brief.» *Congressional Research Service*. October. https://fas.org/sgp/crs/intel/R43765.pdf.

Privacy and Civil Liberties Oversight Board. 2014a. «Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court.» https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

——. 2014b. «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.» https://www.pclob.gov/library/702-Report.pdf.

Privacy International. 2018. «Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards.» http://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global.

Reardon, Joel, Hubert Ritzdorf, David Basin, and Srdjan Capkun. 2013. «Secure Data Deletion from Persistent Media.» In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*, 271–84. Berlin, Germany: ACM Press. https://doi.org/10.1145/2508859.2516699.

Rechthien, Kay. 2016. «Sachverständigen-Gutachten gemäß Beweisbeschluss, 1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestages,» September. https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf.

Renan, Daphna. 2016. «The Fourth Amendment as Administrative Governance.» *Stanford Law Review*, no. 68 (May).

Richardson, Sophie, and Nicholas Gilmour. 2016. *Intelligence and Security Oversight. An Annotated Bibliography and Comparative Analysis*. Palgrave Macmillan. http://www.palgrave.com/de/book/9783319302515.

Schaller, Christian. 2018. «Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden.» *German Law Journal* 19 (4).

Security Intelligence Review Committee. 2018. «SIRC Annual Report 2017–2018: Building for Tomorrow: The Future of Security Intelligence Accountability in Canada.» Ottawa. http://www.sirc-csars.gc.ca/anrran/2017-2018/index-eng.html.

Smith, Graham. 2016. «A Trim for Bulk Powers?» September 7, 2016. https://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html.

——. 2018. «Illuminating the Investigatory Powers Act.» *Cyberleagle*. February 22, 2018. https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html.

Swedish State Inspection for Defense Intelligence Operations (SIUN). 2018. «Årsredovisning för 2017.» February 22, 2018. Stockholm. http://www.siun.se/dokument/Arsredovisning_2017.pdf.

Swire, Peter, Jesse Woo, and Deven R. Desai. 2018. «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft).»

The Chambers of Simon McKay. 2018. «Judicial Approval of Warrants, Authorisations and Notices under the Investigatory Powers Act 2016: A Review of the Investigatory Powers Commissioner's Office First Advisory Note.» 2018. https://simonmckay.co.uk/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/.

Tréguer, Félix. 2016. «From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France,» October. https://halshs.archives-ouvertes.fr/halshs-01306332v11/document.

UK Home Office. 2017. *Interception of Communications. Pursuant to Schedule 7 to the Investigatory Powers Act 2016. Draft Code of Practice*. December 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf.

United States Foreign Intelligence Surveillance Court. 2010. «Rules of Procedure.» Washington, DC. http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

Venice Commission. 2015. «Report on the Democratic Oversight of Signals Intelligence Agencies.» http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

Wetzling, Thorsten (ed.). 2010. *Same Myth, Different Celebration? Intelligence Accountability in Germany and the United Kingdom*. Geneva: Graduate Institute of International and Development Studies.

——. 2017a. «Options for More Effective Intelligence Oversight.» Discussion Paper. https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

——. 2017b. «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls.» Policy Brief. Berlin: Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

——. 2017c. «New Rules for SIGINT Collection in Germany: A Look at the Recent Reform.» *Lawfare*. June 23, 2017. https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

Wissenschaftlicher Dienst des Bundestags. 2017. «Kontrolle von Nachrichtendiensten Bei Zusammenarbeit Mit Anderen Nachrichtendiensten Im Ausland.» March 2017. WD 3-3000-072/17. Berlin: Deutscher Bundestag. https://www.bundestag.de/blob/508038/5a79b26ee2205e08171ee396ef87ae45/wd-3-072-17-pdf-data.pdf.

Wizner, Ben. 2017. «What Changed after Snowden? A U.S. Perspective.» *International Journal of Communication* 11.

Zegart, Amy. 2011. «The Domestic Politics of Irrational Intelligence Oversight.» *Political Science Quarterly* 126, no. 1: 1–25.

List of reviewed Intelligence Legislation

Canada, Bill C-59 (proposed): An Act respecting national security matters (2017). 1st reading June 20, 2017.

France, Interior Security Act (*Code de la sécurité intérieure*).

France, Law No. 2015-1556 on international surveillance (*loi n° 2015-1556 du 30 novembre 2015 relative au mesures de surveillance des communications électroniques internationales*), November 30, 2015.

Germany, Act on the Federal Intelligence Service (*Gesetzt über den Bundesnachrichtendienst*), December 20, 1990, as amended.

Germany, Act on the Protection of the Federal Constitution (*Bundesverfassungsschutzgesetz*).

Germany, G10 Act (*Artikel 10-Gesetz*), June 26, 2001.

Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), July 29, 2009.

New Zealand, Intelligence and Security Act 2017.

Norway, Act relating to the Oversight of Intelligence, Surveillance and Security Service No. 7 (*Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven)*) of February 3, 1995, amended in June 2017.

Switzerland, Federal Intelligence Service Act (*Nachrichtendienstgesetz*), September 1, 2017.

The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*).

United Kingdom, Human Rights Act, 1998.

United Kingdom, Investigatory Powers Act 2016.

United States of America, 50 U.S. Code §1805 – Issuance of Power.

United States of America, Executive Order 12333, December 4, 1981, amended 2003, 2004, and 2008.
United States of America, Foreign Intelligence Surveillance Act of 1978, amended 2008 and 2011.
United States of America, Foreign Intelligence Surveillance Court (FISC), Rules of Procedure, November 1, 2010.
United States of America, Presidential Policy Directive/ PPD 28 – Signals Intelligence Activities, January 17, 2014.
United State of America, Executive Order 13526, December 29, 2009.
United States of America, USA Freedom Act, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, June 2, 2015.
United States of America, US Patriot Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, October 26, 2001.
United States of America, Wiretap Act, codified at 18 U.S. Code §§ 2510-2522.

DEMOCRACY
VOLUME 50

Upping the Ante on Bulk Surveillance

An International Compendium of Good Legal Safeguards and Oversight Innovations

Robust surveillance legislation and effective intelligence oversight can serve as bulwarks against the erosion of fundamental rights in our democracies. Unfortunately, national governments regularly need to be admonished for flaws in their intelligence laws by national or regional courts. Rightly, courts demand more rigorous and effective oversight mechanisms. Yet, given the rapid evolution and the complexity of surveillance technology, what should effective oversight look like in actual practice? Courts will not design oversight institutions or prescribe specific accountability mechanisms. This is the important task of democratic governance that needs to be administered elsewhere.

This compendium by Thorsten Wetzling and Kilian Vieth invites regulatory authorities, oversight bodies and civil society to look beyond national borders and be inspired by the good practices that exist in other countries.

ISBN 978-3-86928-187-2

Heinrich-Böll-Stiftung
The Green Political Foundation
Schumannstraße 8, 10177 Berlin
030 285340 info@boell.de www.boell.de