November 2019 · Kilian Vieth and Dr. Thorsten Wetzling

Data-driven Intelligence Oversight

Recommendations for a System Update

Stiftung
Neue
Verantwortung

Think Tank at the Intersection of Technology and Society

Executive Summary

Intelligence services around the world are driving the evolution of surveillance technology – a rapid, bold, and multi-faceted development. Many countries will run the risk of conducting irrelevant intelligence oversight processes if they fail to incorporate supervisory technology more systematically. The growing volumes of data used in the intelligence sector overwhelm the de facto guarantees of legal safeguards and effective oversight. Modern data analysis entails numerous risks in terms of data abuse and circumventing legal requirements. A lack of up-to-date tools, resources, and technical expertise serves to further undermine effective oversight.

Oversight bodies need an update. They need to adopt tech-enabled instruments to respond to the technological advancements driving the intelligence field. Since key European nations are currently preparing new intelligence reforms, we hope that oversight bodies will embrace a paradigm shift from paper-driven to data-driven reviews.

To advance this process, we would like to propose seven tools for data-driven intelligence oversight that should become part of a reform agenda across Europe. Each tool represents a viable solution to a concrete oversight challenge. Many build upon direct access to operational systems, which enables oversight bodies to conduct unannounced checks as well as (semi-)automated audits on intelligence agencies' data processing. Some of our proposed tools are already being used by intelligence oversight pioneers, while others have been borrowed from good practices in other sectors, such as financial supervision and IT security. The following table summarizes the pressing challenges facing intelligence oversight, coupled with innovations that we feel could effectively meet these challenges.

Oversight challenges ↔ Corresponding tools	
Mystic filter technology: Some intelligence legislation mandates greater data protection safeguards for certain groups. To enforce these types of requirements, agencies carry out data minimization processes, which are critical for legal compliance. However, these filters are rarely submitted to independent checks for accuracy and reliability.	**(A) Data minimization verification** Direct access to the services' stored data enables oversight bodies to test the accuracy of data minimization. This involves scanning the databases with search programs for identifiers (such as phone numbers) that should not be detectable in the filtered data.
Abusive database queries: Cases of illegal and inappropriate intelligence database use can occur when there are insufficient protections in place.	**(B1) Hidden pattern detector** Data analysis software for tracking and visualizing the use of databases. Oversight bodies review log files for potentially suspicious patterns.
Poorly monitored intelligence cooperation: Most oversight bodies lack review mechanisms for ascertaining whether and how national agencies share data with foreign services. Accordingly, these bodies have no control over the use of data that has been shared.	**(B2) Data-sharing alerts** Automated notifications flag critical data sharing arrangements for in-depth review by oversight bodies.
Enforcing retention limits: When analysts or system administrators merge data from sources that do not have the same retention periods, data may remain stored in the databases concerned even after the retention limits have lapsed.	**(B3) Deletion monitor** Deletion activities are recorded in well-structured log files so that oversight bodies can detect outliers in the statistical patterns contained in deletion records.

Trace the use of warrants: Oversight bodies struggle to keep abreast of the large volumes of requests for surveillance measures. They often lack comprehensive digital trails that would make it possible to review the trajectory of authorized data collection and subsequent data use.	**(B4) Authorization tracker** Digital documentation of all warrants and approval decisions allows authorizing judges to detect the simultaneous use of multiple surveillance measures, assess the necessity of new requests and find boilerplate justifications in applications.
Scarce resources: Oversight bodies struggle to systematically decide how to allocate their limited resources effectively and plan their work accordingly.	**(C) Risk assessment** Independent reviewers calculate detailed risk scores for each intelligence systems within their mandate to create a verifiable evidence base for prioritizing oversight tasks.
Opaque agency interaction with private intermediaries: Avoiding over-collection at interception points is critical for preventing rights violations. Oversight bodies do not know enough about this – how can they spot errors such as incorrectly installed bearers?	**(D) Oversight-carrier dialogues** Systematic exchanges between industry players and oversight bodies enable reviewers to track the implementation of data collection. Combined with intermediaries' obligation to report errors, this permits to detect workarounds that undermine legal requirements.

We invite policymakers, intelligence agencies, and oversight bodies to discuss these tools and develop context-specific strategies for data-driven intelligence oversight. In order to successfully implement these tools, we advise oversight bodies not to regard them as substitutes for traditional oversight mechanisms; instead, they should be viewed as necessary additions to existing toolkits and inspection processes.

The hard work of improving oversight will require more than amending existing laws. There has been an overreliance on purely legal solutions to tech-inflicted challenges for too long. This report shows that legal requirements cannot be effectively enforced if the corresponding practical measures are not taken. A concerted effort is thus needed to identify better instruments that complement the legal frameworks and establish accountability.

Acknowledgements

This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation - Project Number 396819157) and by a grant from the Foundation Open Society Institute in cooperation with the Information Program of the Open Society Foundations (Grant Number OR2018 - 45772). The authors are particularly grateful to the members of the European Intelligence Oversight Network (see list of focus group participants in the annex) for their in-depth, constructive feedback on an earlier version of this report. In addition, we would like to thank Giles Herdale, Eric Kind, Jan-Peter Kleinhans, Jörg Pohle, and Félix Tréguer for their valuable comments. We are also grateful for the editorial assistance provided by Sebastian Kostadinov. The authors are solely responsible for the contents of this paper, and the views expressed therein do not necessarily reflect those of the commentators and reviewers.

Table of Contents

Preface

It is not surprising that audit and oversight, in whatever sector, tend to be conservative in their approach. This is very much in common with regulatory processes in general, whether in government or other areas of activity.

This impressive report arising from the European Intelligence Oversight Network will be a very helpful challenge, really raising two interrelated issues. Firstly, how can oversight adapt to keep pace with the rapid technological development of the methods being audited? And secondly, what are the opportunities for using the very latest tools and techniques in the oversight process itself? Both these questions point to important new areas of interdisciplinary research; this is not just about the technology itself, but also about the surrounding legal and ethical frameworks. It is very important that the security organisations themselves, and the oversight bodies and mechanisms, demonstrably work within the rule of law with public and democratic consent.

The report is rich with background information about the current landscape, as well as specific and more general challenges for the future. As the authors say, the question is not if, but how, more powerful data-driven oversight tools can be implemented. They stress the need for oversight bodies to have technical advice from other fields, something provided in small part in the UK by the statutory Technology Advisory Panel to the Investigatory Powers Commission. They also are right that there is no one-size-fits-all solution, and that none of us can deal with this issue on our own.

This foundational report will richly repay careful consideration and reflection, and is food for action as well as thought. I will look forward with great interest to the exciting developments that it will prompt in this important area.

Sir Bernard Silverman FRS
Emeritus Professor, Universities of Bristol and Oxford
Chair, Technology Advisory Panel,
Investigatory Powers Commissioner’s Office (IPCO)
United Kingdom

1. The Need for Oversight Innovation

“Either we adapt to start using new techniques, or we become irrelevant.”[1]
(Paul Killworth, Deputy Director for Strategic Policy, GCHQ)

“Where a power is framed in broad terms in a statute, and oversight is limited to checking if an agency remains within its statutory mandate, then the oversight is of limited use.”[2]
(Venice Commission of the Council of Europe, 2015)

High-tech intelligence vs. low-tech oversight

Intelligence agencies are renowned for driving and adapting to technological change. The vast volumes, velocity, and complexity of the data available to them propels the evolution of surveillance technology. At present, agencies across Europe are deploying an avalanche of new technologies to advance new capabilities such as biometric surveillance and to master long-standing challenges such as information overload. For example, machine learning applications are increasingly coming into play for automated offensive and defensive computer network operations as well as for intelligence analysis and biometric identification.

By contrast, intelligence oversight bodies have been slow and occasionally reluctant to align with and benefit from technological advances. Accountability mechanisms have rarely been considered in research and development for the security sector, and most oversight institutions have failed to bring their pressing needs and challenges to the attention of technologists. The result is widely felt today: Although intelligence agencies are regularly granted expanded surveillance powers[3] and exploit technological innovation, oversight bodies rarely operate with a cutting-edge data-driven toolkit.

The costs of inertia

Clearly, there is a stark discrepancy between the investments in and application of technology within the security sector and the level of investment and tech-savviness commonly found in the oversight landscape. We obviously do not advocate matching all the tax money spent on intelligence with

[1] Babuta, “A New Generation of Intelligence: National Security and Surveillance in the Age of AI,” 19 February 2019, https://rusi.org/commentary/new-generation-intelligence-national-security-and-surveillance-age-ai.

[2] Venice Commission, “Report on the democratic oversight of signals intelligence agencies,” March 2015, para 93, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

[3] In 2019 alone, Finland passed new intelligence legislation, while intelligence reforms that will endow national security and intelligence services with additional surveillance powers are in the making in Austria, Norway, France, and Germany.

investments in oversight measures. That being said, we suspect that most European countries currently spend less than 1 percent of the amount that they invest in intelligence on expanding oversight capacities.[4]

Given the rapid evolution of surveillance technology, this austerity in terms of oversight spending can cost our democracies dearly. The legitimacy of executive conduct depends on effective, modern, and comprehensive intelligence oversight. If oversight bodies are not placed in a position to fully review the practices of intelligence agencies, this will inevitably result in accountability gaps. This in turn provides opportunities for misconduct and abuse which, given the intrusiveness of modern surveillance powers, undermine public trust in the promotion and protection of fundamental human rights.

Fortunately, a number of oversight bodies have recently implemented budget increases and hired tech experts. Nevertheless, few oversight bodies have begun to fully embrace supervisory technology. Instead, many oversight bodies remain over-reliant on paper, and some operate with severe access constraints that prevent them from running more sophisticated audits.[5]

[4] Naturally, this is difficult to express reliably because some budget figures have not been made public. Moreover, the figures that have been made public should be handled with care, as they may not reflect the entirety of intelligence activities. For example, even though the German army's intelligence work represents federal intelligence activity, strictly speaking, it is not typically presented, let alone overseen in the same manner as the three federal intelligence services. Consider the publicly disclosed budget for Germany's federal intelligence agencies in 2018: roughly € 1.4 billion (not including another € 1.4 billion for the new BND headquarters in central Berlin). For oversight expenditures to reach just one percent of this annual intelligence budget, the combined annual budgets available to Germany's fragmented intelligence oversight community (i.e., the Parliamentary Oversight Committee, G10 Commission, Independent Committee, Trust Committee, special units within the Bundestag's administration (PK1-PK4), special units at the Federal Data Protection Authority and within the German Federal Court of Auditors) would have to be at least € 14 million combined. Again, it is difficult to calculate this (due to factors such as the personnel costs for Members of Parliament or the personnel costs within the executive that are needed to respond to oversight requests). The annual budget for the PKGr and G10 secretariat amounted to € 3 million in 2018.

[5] For more elaborate accounts of different factors that impede effective oversight across different jurisdictions, see Goldman and Rascoff, "Global Intelligence Oversight: Governing Security in the Twenty-First Century," 2016; and Wetzling, "Options for more effective intelligence oversight," 2017, https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

Summary table: Why we need oversight innovation

Legitimacy	New security practices require new modes of oversight. If oversight is not rendered fit for reviewing 21st century surveillance, the entire legitimacy of democratic intelligence governance ought to be called in question.
Legality	Courts have called for legal powers to be animated and demanded that bulk interception regimes require effective end-to-end oversight.[6] For example, in the *Big Brother Watch* judgment, the ECtHR's examination of bulk powers identified "first, the lack of oversight of the entire selection process [...]; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination."[7]
Efficacy	Digitization has created an information overload (due to larger datasets, more data sources, inexpensive duplication of data) that needs to be managed. Oversight innovation and supervisory technology enable oversight to be more proactive, reduce reporting costs, and improve the explainability of oversight decisions.

A not-so-new call for action

Since modern intelligence is data-driven, its oversight should be as well. It is time that those whom we trust to ensure that intelligence agencies honor the rule of law and our fundamental rights be rendered fit for fulfilling this task. Unfortunately, this is easier said than done.

On a positive note, there is a growing awareness among European oversight bodies that their current toolkit needs an update. The Dutch CTIVD, for example, embarked on a project called 'Oversight 3.0,' which focuses on the challenge of deletion and prospects for oversight innovation. It is also very laudable that European oversight bodies have ramped up exchange with one another at bilateral and multilateral levels.

Oversight cooperation and innovation have been recognized as crucial topics. It is high time to dig deeper and find out what automation and supervisory technology can do to address current oversight challenges. Else, the ubiquitous call for more effective oversight instruments will remain rather diffuse and

[6] Smith, "What will be in Investigatory Powers Act Version 1.2?," 30 October 2018, https://www.cyberleagle.com/2018/10/what-will-be-in-investigatory-powers.html.

[7] European Court of Human Rights, "Case of Big Brother Watch and Others v. The United Kingdom," 13 September 2018, http://hudoc.echr.coe.int/eng?i=001-186048.

inconclusive. We believe that this can be broken down into more tangible parts. Moreover, there are numerous specific ideas that have yet to be earnestly discussed among those who wish to change the status quo.

The aim of this paper

In writing this paper, which represents a feasibility study of sorts, we hope to contribute toward this important goal. More concretely, we have presented and discussed a range of viable tools for enabling more data-driven intelligence oversight. If these are implemented, we believe that they can help oversight bodies keep track of modern surveillance and establish accountability.

We are aware that the institutional design of oversight in certain countries is subject to its own path dependencies and particularities. Despite these factors, the relevant question is not *if* but *how* more powerful data-driven oversight tools can be implemented. Of course, these are matters that oversight bodies cannot solve on their own – they need technical advice from other policy fields and the realm of business. Moreover, since these considerations clearly touch on oversight-executive relations, intelligence services and their executive control must be included in the conversation.

As members of civil society, our capacity to influence oversight bodies to wake up to the challenges at hand and begin answering the call for oversight innovation in earnest is limited. We document what is possible and what is being practiced in an attempt to provide decision-makers with greater argumentative backing.

Given the highly varied landscape of parliamentary committees, judicial oversight, expert bodies, and data protection offices, there cannot be a one-size-fits-all solution. However, we hope that interested readers from all sectors will engage creatively with our proposals.

A note on our method

As part of our quest for ideas and suitable applications for addressing common oversight challenges, we conducted desk research as well as a series of semi-structured interviews with practitioners in the fields of data-driven policing, financial supervision, and data protection. A large part of this paper builds upon the direct access to operational systems and data that a minority of intelligence oversight bodies across Europe now enjoy. Our basic ideas were tested and refined during a workshop of the European Intelligence Oversight Network in May 2019.[8]

Roadmap

In response to specific oversight challenges, the next chapter introduces and elaborates on a range of ideas and applications for positive change. This is followed, in Chapter 3, by a discussion of key concerns – such as information security, executive privilege, and duplication – that these tools need to address. Afterwards, we reflect on where these tools might best be situated, i.e., their proximity to the executive. Finally, we offer recommendations on how to advance the implementation of these ideas.

As we will explore, modes of implementation can vary in terms of how conservative or progressive they are, and there are good arguments for prioritizing some tools over others. By and large, however, we will argue that data-driven intelligence oversight promises increased effectiveness and greater legitimacy at reduced costs – provided that oversight bodies acquire and make better use of their growing access to the operational systems of the intelligence services.

[8] Stiftung Neue Verantwortung, “Second Workshop of the European Intelligence Oversight Network.” 10 May 2019, https://www.stiftung-nv.de/en/event/second-workshop-european-intelligence-oversight-network.

2. Updates to the Oversight Toolkit

> *"The CTIVD explores the use of computerized data processing in oversight itself, e.g. by automatically comparing the data processed by the services, with the aim of being able to recognize any processed data deviating from the standard."*[9]
> (CTIVD Annual Report 2018)

Intelligence agencies today process more data than ever before, and there is no indication that this will stop anytime soon – quite the contrary, in fact. This in turn creates a pressing need for intelligence oversight bodies in Europe to catch up to technological change and the rapid evolution of the surveillance trade. In this study, we identify and discuss a range of applications and mid-term objectives that we feel should be incorporated into an oversight reform agenda across Europe.

Before elaborating further on the prospects of end-to-end predictive oversight, we need to unpack a few elements. The following section starts by defining and defending our point of departure. We then explore whether and how the data-driven audits we present are suitable for independent intelligence oversight bodies. Put differently, are there applications that should reside exclusively within the institutions of internal and executive control, i.e., remain confined to the corridors of executive power? Finally, we put supervisory technology in perspective by stressing the equal importance of human-led inspections.

Our point of departure: Direct access to intelligence services' operational systems

Some European intelligence oversight bodies now claim to possess more comprehensive access to the operational systems of national intelligence services. Yet, few oversight bodies have made detailed public statements about the implementation of their access. That is why our assertions on access are based on semi-structured expert interviews with employees of review bodies in the European Intelligence Oversight Network as well as desk research regarding the latest public reports published by the oversight bodies.

However, we can say on the basis of our sources that, despite notable differences, each of the review bodies listed below has acquired an access level

[9] Dutch Review Committee on the Intelligence and Security Services, "Annual Report 2018," p. 15, https://english.ctivd.nl/binaries/ctivd-eng/documents/annual-reports/2019/06/20/index/CTIVD+annual+report+2018.pdf.

that is qualitatively different from what the majority of their European peers have. This now calls for the introduction and refinement of supervisory technology.

For the purpose of this report we characterize their access level as "direct access." By this we mean, overseers can log into the operational systems of the intelligence services and retrieve and analyze independently specific datasets of their own choosing. This said, direct access for us should not be equated with full access. Some access restrictions that the agencies used to maintain the security and secrecy of their system are likely to remain in place when overseers access operational systems.

Statutory specifications, the ways in which these are interpreted, the technical equipment involved, and its practical setup vary from country to country. Some have decided to provide overseers with dedicated "oversight" computer terminals at the premises of the intelligence services. This mode of on-site access is used, for instance, by the British,[10] Norwegian, and Danish oversight bodies. Under this setup, for example, UK oversight officials may, in addition to their regular examination of the system, instruct agency staff to extract data and export it to another system (for example, as a spreadsheet) to enable a more detailed examination and analysis to be undertaken and also maintain the integrity of the operating system. Other oversight bodies may log in remotely from their own offices. For example, the Swiss oversight body AB-ND enjoys remote access to the data stored by the intelligence service NDB, including specially protected personal data.[11] Another distinction of the type of access is whether inspectors enjoy permanent access to IT systems and intelligence databases, or are granted access on a case-by-case basis for a limited time span or a specific investigation.

[10] IPCO's published 2017 annual report to parliament states that "[d]uring inspections, our inspectors have access to the system used by investigators and analysts at MI5 to apply to access the bulk communications data and we undertake random sampling and run query-based searches on the system. For example, inspectors might use the system to show us every application which included the word 'journalist'. This means that our inspectors can (i) evaluate the analysts and investigators' necessity and proportionality considerations; (ii) examine particular operations; and (iii) identify requests for more sensitive data sets or those requiring data over longer time periods." See IPCO, "Annual Report 2017," January 2019, p. 66, section 9.32, https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190131.pdf.

[11] Federal law for the Swiss Intelligence Agency (NDG), "Functions, Right to Information and Recommendation of Oversight. Art. 78 (5)," 25 September 2015, https://www.admin.ch/opc/de/federal-gazette/2015/7211.pdf.

Based on our definition of direct access, we believe the following European oversight bodies meet the criteria:

- Denmark: Intelligence Oversight Board (TET)[12]
- Netherlands: Review Committee on the Intelligence and Security Services (CTIVD)[13]
- Norway: Parliamentary Oversight Committee on Intelligence and Security Services (EOS)[14]
- United Kingdom: Investigatory Powers Commissioner's Office (IPCO)[15]
- Sweden: Inspectorate for Defense Intelligence (SIUN)[16]
- Switzerland: Independent Oversight Authority for Intelligence Activities (AB-ND)[17]

Given the difficulties we encountered to amass falsifiable information on access levels, this list cannot claim to be exhaustive. We invite other oversight bodies to come forward and report on their access level.

Direct access to operational systems has the potential to be game-changing in that it enables oversight bodies to carry out random checks, unannounced inspections, and (semi-)automated controls on intelligence agencies' data handling. Direct access reduces the dependency of oversight bodies (both internal and independent) on information provided by intelligence services. This approach is also likely to heighten intelligence services' incentive to comply because intelligence officials will not be able to know whether a given matter will be reviewed.

Naturally, direct access will not eliminate all barriers to data. Intelligence agency employees are commonly subjected to access restrictions: They do not have access to *all* kinds of data, in theoretical and practical terms. Even senior staff are bound by classification levels and the "need-to-know" principle. It is therefore difficult to fathom how oversight bodies could fully surpass these restrictions.

Bearing this in mind, the crucial question concerns what *types of data* overseers can *actually* access and how. A specific oversight tool or audit practice may typically require access to a certain subset of intelligence data. The table

[12] https://www.tet.dk/?lang=en

[13] https://english.ctivd.nl/

[14] https://eos-utvalget.no/en/home/

[15] https://www.ipco.org.uk/

[16] http://www.siun.se/

[17] https://www.ab-nd.admin.ch/de/home.html

below distinguishes between various access types needed for different oversight functions. It would be premature to deny the need and feasibility of direct access in general. Instead, the focus should lie on the specific types of data that are needed for effective internal and external intelligence oversight.

Type of data access	Characterization	Benefits for proposed tools
Access to source data	The "raw" data that has not been processed for later use. Its attributes depend on the source of the data, such as cable interception, open sources, human sources, acquisition of datasets, hacking operations, sensors, and reconnaissance satellites.	(C) Risk assessment (B4) Authorization tracker (D) Oversight-carrier dialogues
Access to stored data	Structured databases that contain data after the "minimization" process. This comprises both metadata and content.	(A) Data minimization verification (C) Risk assessment
Access to log files	Metadata on intelligence agencies' use of data, including selection, triage, transfer, deletion, and assessment activities.	(B1) Hidden pattern detector (B2) Data-sharing alerts (B3) Deletion monitor (B4) Authorization tracker
Access to finished intelligence (FININT)	The outputs of the intelligence process, often directed at decision-makers. Finished intelligence products include reports on specific threats, countries, military operations, etc.	(B4) Authorization tracker (C) Risk assessment

Direct access: Vice or virtue?

By conducting a series of practitioner interviews with members of European oversight bodies with direct access to intelligence services' data, we learned how oversight can become far more effective if this comparatively more comprehensive access is used in conjunction with modern supervisory technology. A wide range of important review and audit tasks could be supported by tools that we think would render the work of inspectors more efficient.

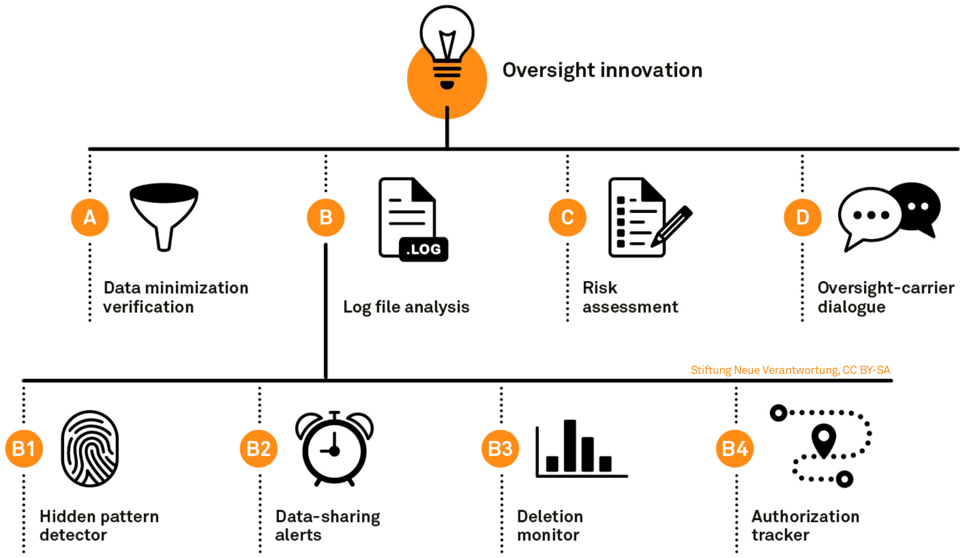
That being said, how would these more rigorous data-driven audits figure within the context of democracy? While few would argue against the need for compliance audits, many countries remain undecided as to whether these audits should be solely conducted by internal and executive oversight institutions operated by the government (Position 1) or whether they ought to be administered by independent oversight bodies as well (Position 2). We will return to this question at several points throughout this report. It is an important one, with practical ramifications. Consider, for instance, the fact that some oversight bodies, such as TET, are independent and have direct access to operational systems, whereas others, such as the G10 Commission and the German Federal Data Protection Authority, do not currently benefit from this kind of access.

There are numerous arguments and concerns that need to be addressed when it comes to granting oversight bodies greater access. These include IT and cybersecurity concerns, the principle of executive privilege, and practical aspects such as the risk of oversight duplication. Moreover, the need for supervisory technology needs to be reconciled with the limited resources oversight bodies typically have. Each of these points merits careful attention. We will return to them in Chapter 3, after we have elaborated on new tools introduced in response to common oversight challenges.

Technology cannot be the answer if you do not understand the question
In advocating more data-driven intelligence oversight, we recognize and encourage the essential role played by dedicated inspectors who sift through files and probe service members on a wide range of intelligence governance matters. We believe that direct support, further investments, and a reliance on human experience and analysis remain crucial to fostering effective oversight in the 21st century. Combining data-driven oversight methods with human analysis and interpretation is necessary to achieve genuine innovation. Accordingly, we would like to call upon inspectors and oversight professionals to make greater use of data-driven oversight, recognizing this as a key part of their growing toolkit.

We would also like to caution against dogmatic beliefs in algorithms and data as a one-size-fits-all cure for current challenges. Databases and data collection practices are man-made; as such, they contain, and can even at times exacerbate, inaccuracies and biases that can easily skew findings and decisions in the absence of human awareness and corrective measures.

Overview of the tools



We will now introduce the tools, applications, and ideas that we believe should be discussed more prominently by those responsible for ensuring effective democratic intelligence oversight and accountable intelligence services. We will start by identifying and discussing a particular challenge that oversight bodies typically face, and will then present an idea or a tool that can serve as a potential response to said challenge. The image below summarizes the various innovative methods and tools discussed in this section. Of course, no discussion of policy recommendations is complete without mentioning the advantages, disadvantages, and risks that they may entail. We will address these in Chapter 3.

A. Monitoring stored data for filter errors

Challenge

History is replete with cases in which practical application on the ground did not follow the rulebook. Ensuring that legal provisions are actually upheld and not “creatively” (or inadvertently) circumvented in practice poses a tremendous challenge for any institution charged with reviewing large-scale bureaucratic systems. To name a related example, we have noted that some European intelligence laws provide higher data protection safeguards for nationals than for non-nationals or foreigners abroad.[18] Some laws provide extra safeguards for the interception of communication that relies on confidentiality (e.g., the electronic communication between patients and doctors, churchgoers and priests, or clients and lawyers). These and other specific conditions must be met in order for intelligence practice to remain lawful in the respective country. Many agencies perform complex data minimization processes in order to fulfill these and other requirements.

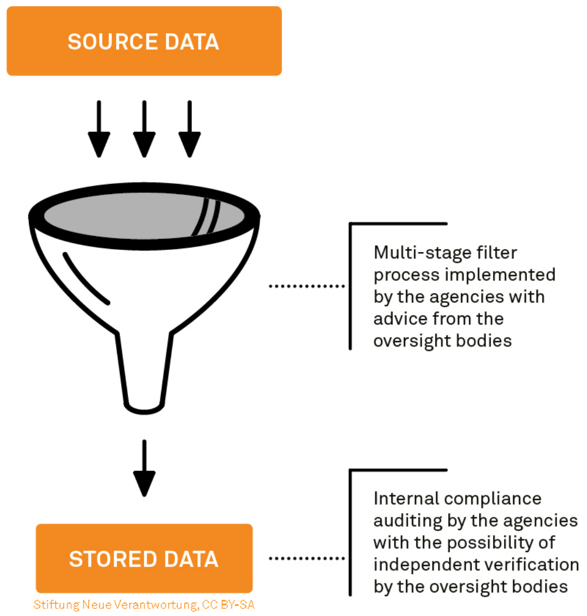
When it comes to critical information regarding the accuracy of data minimization processes, many intelligence oversight bodies in Europe often have no choice but to rely on the information that they receive from government or intelligence agencies. Genuine reviews of the accuracy of the filters that agencies use to comply with legal safeguards are rarely conducted.[19] This poses a significant problem; after all, a huge volume of data might be processed incorrectly if the filters are not working properly. Moreover, a wide range of legal provisions need to be upheld by data minimization procedures; failure to conduct sufficient reviews makes it difficult to ascertain whether said procedures are actually compliant. As such, oversight bodies would be well advised to strive for greater independence in reviewing and verifying data minimization processes. Parliaments should incorporate provisions into intelligence laws to indicate what filters should achieve during the data collection phase.[20]

[18] For a detailed discussion on the role of nationality in intelligence legislation, see the report by Swire, Woo, and Desai, "The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance," January 2019, Aegis Series Paper No. 1901, https://www.hoover.org/sites/default/files/research/docs/swire-woo-desai_the-important-justifiable-constrained-role-of-nationality-in-foreign-intelligence-surveillance1.pdf. The German constitutional court is scheduled to pronounce on the legality of the 2016 BND Law that introduced different types of data protection based on nationality.

[19] One such exception is the recent CTIVD report on the application of filters in "research assignment oriented" (OOG) interceptions by the Dutch intelligence services AIVD and MIVD (our translation), which is available in Dutch via the Review Committee on the Intelligence and Security Services, "Progress Report," 17 July 2019 (CTIVD Nr.63), https://www.ctivd.nl/documenten/rapporten/2019/09/03/index.

[20] For further information on filters and data minimization programs, see Wetzling and Vieth, "Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations," November 2018, pp. 53-56, https://www.stiftung-nv.de/sites/default/files/2019_hrc_annex5_compendiumbulksurveillance.pdf.

Idea: Data minimization verification


SOURCE DATA
Multi-stage filter process implemented by the agencies with advice from the oversight bodies
STORED DATA
Internal compliance auditing by the agencies with the possibility of independent verification by the oversight bodies

Stiftung Neue Verantwortung, CC BY-SA

If oversight bodies were to be provided with access to intelligence services' stored data, they could design (or work with intelligence agencies to co-design) tools for testing the accuracy of data minimization programs. For example, reviewers could produce lists of search terms such as identifiers for protected groups of persons, or the names or email addresses of nationals working for international organizations. Based on national intelligence laws, reviewers could also specify indicators that would point to a violation of a specific legal safeguard. An automated search program could then scan the entirety of stored data for identifiers that should not be detectable after a filter has been applied.

Discussion

Intelligence agencies are typically responsible for implementing filter systems. Whether or not filters and data minimization programs fulfill their purpose is, however, also a question of immediate concern for independent oversight bodies. Flawed data minimization could lead to wide-scale infringements of fundamental rights which, in turn, would severely undermine the legitimacy of government conduct. Direct access to intelligence databases would allow oversight bodies to independently search for remnants of data points that should have been filtered out, such as domestic data in foreign intelligence databases.

How should oversight bodies be involved in data minimization verifications? This verification process could be (partially) automated with validation scripts: As a standard routine, computer programs could search databases to verify that stored intelligence data complies with the applicable data minimization rules. Testing the compliance of stored datasets could involve simple measures such as allowed character checks: For instance, it might be stipulated that a phone number in a foreign dataset should not contain the domestic country code or the identifiers of national citizens working for international organizations. Overseers could also work with lists of search terms that they deem relevant without disclosing said terms to the intelligence service. Over time, oversight bodies engaging in these practices would be able to draw conclusions on the overall accuracy and legality of the filter process and subsequently advise lawmakers on the extent to which legal safeguards for certain data categories are successfully implemented in practice.

Allowing oversight bodies to run validation scripts on stored data will require negotiations with the executive, because these checks might constitute undue duplication. Moreover, in light of the resources and technological expertise available to oversight bodies, it might also be unrealistic to demand that oversight bodies run the full gamut of compliance testing – most intelligence agencies are already doing this because of their obligation to follow the law. However, it would be a mistake to exclusively rely on the information provided by intelligence agencies without subjecting this to any independent verification. We therefore believe that oversight should recognize data minimization as a crucial intelligence practice that merits critical independent review. Oversight bodies should be consulted accordingly when it comes to designing and implementing data minimization processes. Furthermore, oversight bodies should be permitted to run independent compliance audits on the data stored by intelligence services. This would amount to a reverse extension of the UK's double-lock approach,[21] whereby warrant authorization as well as data minimization will now require input from independent oversight bodies.

In keeping with this practice, data analysts working within oversight bodies could pick specific subsets of data that need to abide by relatively easy binary categories – for example, tests based on fairly straightforward numeric indicators such as country codes in phone numbers and text messages.

[21] The UK's IP Act introduced "a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these (and other warrants) cannot come into force until they have been approved by a judge." See Government Communications Headquarters, "Investigatory Powers Act," 18 March 2019, https://www.gchq.gov.uk/information/investigatory-powers-act.

Analysts could then proceed step by step towards more difficult verification that involves multiple, potentially overlapping data protection categories such as national citizens working abroad in protected professional fields.

B. Log file analysis: How to make better use of audit trails

> *"Analyzing log files is an important tool and it's hard to do oversight without it. Our experience is that it's necessary to validate the log files. In other words, overseers must check the logging tools to make sure that the logs are complete and correct."*
> (Emil Bock Greve, Head of Secretariat,
> Danish Independent Oversight Board)

Intelligence and security agencies rely on large IT systems to organize and make sense of the vast amounts of data they collect. Contractors or in-house units provide integrated software solutions for data analytics.[22] These types of information technology systems produce enormous amounts of metadata (often by default) that are recorded in log files. As we will illustrate in further detail below, this information has the potential to substantially empower internal audits as well as independent intelligence oversight bodies.

Agencies constantly review log files. They have far more experience and expertise in log file analysis then oversight bodies currently do. As a result, alongside unanswered questions concerning executive privilege, entrusting oversight bodies with various tools for log file analysis carries a significant risk of task duplication. However, as noted in the preceding section of this report, this risk needs to be weighed against the risk of over-dependence on intelligence services' internal audit processes, some of which we know to have been underperforming or, even worse, to have been ignored by decision-makers in the intelligence community.[23]

Preface on log files

Log files reveal when, how, how long, and by whom a given system is used. All changes made to a dataset and all queries performed by a certain user can

[22] For example, cross-system information analysis platforms such as Palantir's Gotham, Rola's rsIntCent, or IBM's i2 Analyst's Notebook. Some governments also systematically invest in the development and delivery of cutting-edge technologies to their intelligence agencies via organizations such as I-Q-Tel (https://www.iqt.org/) and Defense Advanced Research Projects Agency (DARPA, https://www.darpa.mil/) in the United States.

[23] For example, the German Chancellery publicly addressed technical and organizational deficits in the wake of the NSA affair, which led to an inquiry committee that provided further information on those deficits. Lohse, "Kanzleramt übt heftige Kritik an BND (German Chancellery heavily criticizes BND)," 23 April 2015, https://www.faz.net/aktuell/politik/inland/kanzleramt-uebt-heftige-kritik-an-bnd-13555622.html.

be stored and automatically tagged with timestamps. This provides system administrators and designers with valuable data for restoring files, recovering incomplete transactions, and developing the software's user experience. The following events or actions are typically recorded in log files, which render them particularly useful for audit purposes:

- Alterations or modifications of data points and datasets
- Time and duration of activity and access
- User identification (including location data, for example)
- Attempted/failed actions on particular databases

For example, if a user adds or deletes a file in a database, the corresponding log file would contain metadata that captures the user's ID, the time of the change, and the type of data that was changed. Automated transactions such as the pre-scheduled deletion of datasets would also be recorded in log files.

Log files normally form static datasets that chiefly enable ex-post reviews. If permanent access to log files does not exist, audit data may also be "pushed" periodically from the IT system of an intelligence service to that of an oversight body as a form of automated reporting. Conversely, oversight bodies can also "pull" data, either manually or automatically, from a supervised agency.[24]

The table below summarizes the potential advantages of directly using the operational systems of intelligence agencies as opposed to analyzing exported copies of datasets. Effective oversight, as practitioners point out, ideally makes use of both types of data access.

Advantages of using the operational systems of intelligence services for log file analysis	**Advantages of using "offline" copies of datasets for log file analysis**
Controls on ongoing operations, not just ex-post reviews.	Once a log file is exported, no "after the fact" adjustments or tampering are possible.
Inspectors can react more quickly to detected irregularities.	Inspectors have more autonomy in using audit data; for example, they can choose their own analysis software.

[24] Following the principle of data reduction, oversight bodies need to carefully consider which records they need to keep on their own premises or IT systems if the same records are already stored within the issuing agency or ministry.

Audit trails are potentially more up-to-date, complete, and well-structured.	Oversight activity does not interfere with operational systems.

Oversight bodies working with offline copies of log files have confirmed that there can be fundamental differences in the quality of the information that they retrieve from these files. If a log file merely contains information such as “file changed” without including further information about the type of changes, when these changes were performed, and who performed these changes, then the logs, taken on their own, do not provide the kind of granularity that is necessary for genuine oversight.

Interestingly, recent legal reforms may have introduced more specific obligations to grant oversight bodies access to protocols and registries. However, the quality of log file data, which represents an equally important factor in compliance audits, still tends to go overlooked. Moving forward, applications for data analytics performed by the intelligence community should be designed so that data use is recorded in enough detail for auditors to be able to fully comprehend the practice in question. At present, there is still a great information asymmetry in terms of what log files reveal to internal auditors and independent oversight institutions.

Depending on the practical implementation, oversight access to log files can create ample room for novel applications, which we will discuss below.

B1: Engaging in more systematic pattern identification

Challenge

Intelligence services such as the GCHQ, DGSE, and BND collect and store an ever-growing amount of data. It is in the interest of intelligence agencies serving open societies to have effective compliance and oversight mechanisms in place. Data protection starts with proper access rights management and compliance mechanisms that are built into intelligence agencies’ information systems. For example, if a user selects data for an outright inadmissible examination, or if agents try to use data for an entirely different purpose than that which was originally approved, then the agencies’ operational systems should automatically block this behavior.

Despite the recognized need for and importance of data protection, alarming cases of illegal and inappropriate intelligence database queries have surfaced.[25] Cases in which police officers have queried databases containing sensitive personal information for private purposes are more commonly reported.[26] These are not isolated events; effective safeguards against abusive database queries are often lacking. This points to the need for independent oversight bodies to take more action. For example, they could review log files for unusual access times or deletion patterns, or exceptionally high frequencies of queries for given files.

Idea: Hidden pattern detector

What kinds of patterns might point to activities that may not be legally compliant? For instance, reviewers may be inclined to look out for unusual peaks in the activity of an individual user (such as an intelligence analyst) or exceptionally high numbers of transactions in a specific file. Reviewers could also keep an eye on potential issues, such as particularly high numbers of user accounts that triage certain data, and scan logs for exceptionally frequent use of databases from uncommon access points. Options for analyzing log files range from simple descriptive methods (that build on distinctions between average, median, maximum, and minimum values) to sophisticated machine learning or statistical analysis techniques. Based on log files, data analysis software can help overseers visualize the use of databases by intelligence analysts, and detect and illustrate statistical correlations and networks from the logs. If auditors manage to identify patterns of non-compliance or illegal data use, they can then decide to start an in-depth investigation of the respective IT system or of the responsible employee's activities. To avoid making misguided accusations, some software tools also make it possible to recreate the exact chronological sequence of searches and other actions. This enables auditors to perceive the intelligence analysis process through the eyes of a given user. Some initially suspicious user behavior might appear rational and compliant when reproduced in this way.

[25] A declassified FISA court ruling showed how the FBI abused NSA's bulk surveillance data by looking up online communications of U.S. citizens, including those of FBI employees and their family members. According to the FISC report, the FBI ran about 3.1 million searches related to U.S. persons in 2017 alone. At the same time, the FBI only refers about 10,000 investigations per year. See: Aaronson, "A Declassified Court Ruling Shows How The FBI Abused NSA Mass Surveillance Data," 10 October 2019, https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/; original FISC document at: United States Foreign Intelligence Surveillance Court, "FISC Opinion regarding the Section 702," 18 October 2018, https://www.documentcloud.org/documents/6464604-2018-FISC-Ruling-Shows-How-FBI-Abused-NSA-Mass.html.

[26] For a collection of police database abuse in Germany, see: Golla, "Neugier und Datenkriminalität," 16 August 2019, https://www.lto.de/recht/hintergruende/h/polizei-datenbanken-missbrauch-datenkriminalitaet-abfragen-daten-schutz/. For a recent case in the UK, see Corfield, "London Cop illegally used police database to monitor investigation into himself," 11 July 2019, https://www.theregister.co.uk/2019/07/11/met_police_sgt_pleads_guilty_computer_misuse_crimes/.

Obviously, if the log files only record user activity with a minimum of detail (e.g., “file has been read, file has been saved, file has been changed”) without including more granular information, this will significantly reduce the opportunities that log file analysis can open up for oversight purposes.

Which pattern detection methods will yield the best results for auditing purposes? This depends on the available data and the purpose of the oversight investigation in question.[27] Audits can reveal what types of data analysts typically use in tandem, such as cell phone locations and open source intelligence (OSINT) or social media intelligence (SOCMINT), possibly in conjunction with voice recognition and data visualization software. This can often lead to the retention of data in new databases that may not sufficiently adhere to legal requirements (as regards purpose limitations or data sharing restrictions, for instance). By tracing the use patterns of a specific tool, oversight officials may also arrive at a better, evidence-based general understanding of the actual work routines carried out by analysts within intelligence services. Understanding “normal” usage can then allow oversight officials to hone in on potentially suspicious activities. Pattern detection in log files can therefore be regarded as a means of improving dialogue: It can help target the right people whom overseers should contact for in-depth investigations.

Configuring log file pattern analysis as described above requires precision and technical prowess. It also entails the (large) risk that broad search patterns might produce too many false alerts, which could overwhelm oversight bodies and distract them from more important tasks. Moreover, an overly specific search might produce no alerts at all (even if these might be merited) if the notification mechanism is configured to combine too many search parameters.

Given that there can be hundreds of users in a specific system and millions of individual actions recorded per year, effective oversight cannot rely on manual analysis alone. (Semi-)automated analysis can allow reviewers to better cope with vast volumes of logs. Interestingly, the IT security community faces the same challenge when it comes to reviewing logs (for intrusion detection systems). Oversight bodies would do well to look into the wealth of research conducted by information security companies and computer scientists on how to best analyze logs as well as how to cope with “attention fatigue” caused by reviewing ever-increasing log files.

[27] For example, financial auditors seek to detect insider trading activities or money laundering. IT security departments try to track network intrusion. For many companies that handle large amounts of data, such as banks and insurance companies, robust compliance systems are essential for ensuring efficient operations.

B2: Consistently scanning transferred intelligence

Challenge

Intelligence cooperation, be it at the national or at the international level, has become more significant and ubiquitous over the past few decades. While it is clearly important for national security agencies to establish and maintain robust liaisons with their international partners, this domain of intelligence practice remains the least effectively overseen. It can invite collusive delegation and creative non-compliance.[28] In the absence of genuine attempts at international oversight cooperation,[29] democratic deficits and accountability gaps will continue to increase.

While intelligence cooperation is often referred to as the "hardest nut to crack" in the already complex and difficult pursuit of democratic intelligence, improvements to the status quo are nonetheless possible.[30] Unfortunately, though, most intelligence oversight bodies lack the knowledge and review mechanisms to ascertain whether and how national intelligence agencies share data with foreign intelligence agencies.[31] One of the core problems is that when intelligence agencies share data with foreign partners, they often lose control over the subsequent use of said data.

This lack of control is problematic for a wide range of reasons. For instance, the transferred information may be used for a different purpose than that which was originally foreseen, or data may be acted upon by security agencies with executive powers. Just because an agency may lose control over the use of their data by their partners does not mean that the individual ceases to have rights or that oversight bodies should stop holding the

[28] The collusive delegation thesis depicts the democratic deficit of intergovernmental cooperation not merely as a "by-product of the transfer of powers [...], but also one of the purposes of this transfer." According to this thesis, states can cooperate against societies by pooling "their authority in order to loosen domestic political constraints." Koenig-Archibugi, "International Governance as New Raison d'état? The Case of the EU Common Foreign and Security Policy," 2004, European Journal of International Relations 10 (2), 147-188.

[29] Wetzling and Vieth, 2018, p. 62f.

[30] For an interesting collection of arguments in favor of greater state obligations and adequate control systems for joint intelligence databases, see Ryngaert and van Eijk, "International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees," 2019, International Data Privacy Law 9 (1), https://academic.oup.com/idpl/article/9/1/61/5427456.

[31] On a positive note, "examination warrants" have been introduced under the UK's IP Act: These mean that the government must seek independent judicial approval from an Investigatory Powers Commissioner (a judge) before selecting content for examination. This also applies to the examination of data shared by foreign intelligence services. For a more detailed discussion, see: Smith, 2018.

executive accountable. At present, intelligence law and oversight practice include severe limitations on the effective review of data-sharing.[32]

Idea: Data-sharing alerts

As is the case with other notifications that oversight bodies could receive from more advanced audit systems, one could imagine a software that automatically scans log files for activities indicating problematic intelligence sharing. This would require log files that include meaningful information about data-sharing so that data transfers become auditable. Consider, for instance, an agency that shares a database with another service bilaterally, or an agency that submits data to a joint database hosted in another country: Some oversight bodies are mandated to review whether information that their national service shares with foreign agencies abides by legal requirements. This type of data-sharing can involve large volumes of data, as well as highly sensitive personal information.

A more consistent and rigorous review of log files may reveal that certain databases used for intelligence cooperation do not effectively implement the relevant data protection requirements. In Germany, some of these requirements must be put into writing in "database establishing orders." These orders may include checks on compliance with "consolidated guidance," such as ensuring that information sharing does not lead to torture.[33] Oversight bodies charged with auditing data processing can also systematically review whether a database that is administered by a national intelligence agency for the purpose of cross-border intelligence sharing complies with legal requirements.[34]

[32] For example, the German Independent Committee is authorized to perform random checks to verify that no data that violates the ban on industrial espionage (Section 6 (5) BND Law) and no data that may counter Germany's national interest is being shared (Section 15 (3) BND Law). However, the Independent Committee lacks the technical equipment and access to selectors and data minimization reports necessary to effectuate this oversight function. The German DPA faces a similar dilemma: It is entitled to examine the database arrangement of joint databases run by the BND and the data that the German agency submits to these databases. However, the law is bound by several limitations. According to Section 28 BND Law, the German DPA may only review joint databases that are run by the BND (Section 27 BND Law), and even these reviews are constrained; they can only be carried out on the database arrangement and the data that the German intelligence services have added to the joint database under their own auspices. As a result, the majority of joint foreign databases to which German intelligence services contribute, as well as the BND's processing of data in joint foreign databases, fall beyond the remit of the German DPA.

[33] Perraudin, "Mordaunt pledges to review internal MoD torture guidance," 20 May 2019, https://www.theguardian.com/uk-news/2019/may/20/mordaunt-pledges-to-review-internal-mod-torture-guidance.

[34] See, for example, the report by the CTIVD on the CTG exchange infrastructure regarding personal data on alleged jihadists. Dutch Review Committee on the Intelligence and Security Services, "Review report 56 on the exchange of personal data on (alleged) jihadists by the AIVD," (CTIVD Nr. 56), https://english.ctivd.nl/investigations/r/review-report-56-on-the-exchange-of-personal-data-on-alleged-jihadists-by-the-aivd.

Oversight bodies should be involved in the development of informative audit trails for data-sharing, which would include acting as independent reviewers of intelligence agencies' internal compliance processes and the implementation of these in the agencies' IT systems. Operational systems for data-sharing should prompt the confirmation of appropriation requirements. If an agency has shared intelligence that was tagged for special protection, than this protection must be communicated to the recipient of said information. Routine audit scripts might flag these types of particularly critical cases for in-depth review by oversight bodies.

Intelligence agencies might liaise with agencies that are known for disrespecting human rights, and foreign services might ignore the specific demands of their cooperation partners.[35] Because of this, the Netherlands uses a system of so-called weighting notes whereby the risk associated with intelligence partners abroad is assessed in accordance with five criteria.[36] To enhance the utility of these weighting notes, the risk level associated with foreign intelligence agencies could be turned into structured metadata within the intelligence service's operational system. Auditors could then automatically detect and flag data-sharing with high-risk partners. This in turn would provide a solid basis for planning further in-depth inspections and auditing critical data-sharing arrangements more systematically. It would also make it possible to prioritize the review of data-sharing with foreign intelligence partners.

B3: Analyzing data deletion statistics

Challenge

European intelligence laws stipulate different retention periods for different types of data. For example, in France, evaluated content data from foreign intelligence intercepts can be kept for 12 months, whereas metadata from foreign collection can be kept for 6 years.[37]

What happens after a retention period has lapsed? Data deletion continues to pose an enormous challenge for intelligence services and oversight bodies

[35] For example, the German BND cooperates with more than 450 different intelligence services worldwide. See Becker and Schulz, "Wieviel Geheimdienst braucht Deutschland?," 16 November 2016, https://www.swr.de/film/bnd-schattenwelt-geheimdienst-doku-nachrichtendienst-swr/-/id=5791128/did=17666664/nid=5791128/1o343xj/index.html.

[36] These include the "democratic embedding" of the receiving agency, its professionalism and reliability, the legal powers and capabilities of the service, and the level of data protection that is ensured. The weighting notes are subject to review by the CTIVD. See Wetzling and Vieth, 2018, p. 26.

[37] For an overview of selected retention periods set out in foreign intelligence laws for different data categories, see: Wetzling and Vieth, 2018, p. 56.

alike.[38] In order for data to become irretrievable, the physical records on a storage medium must be overwritten with other data several times. Proper deletion can therefore become more costly, time-consuming, and complex than data storage itself. Nevertheless, data retention periods and deletion regulations have been codified into national surveillance legislation and ought to be adhered to in practice. If that is not feasible, than there should at least be a debate as to why this cannot be guaranteed in practice and what safeguards are needed to make sure that data retention does not facilitate data abuse. Having said this, there may be a risk that overly strict deletion requirements will prompt the extension of deletion periods.[39]

Once data storage periods have lapsed, deletion is usually carried out in an automated manner that rarely requires manual intervention. Data retention issues frequently arise, however, when analysts or system administrators merge data with data from other sources that do not have the same retention limit. Moreover, if data gets moved to an analysis environment without built-in automatic deletion, it may never get deleted.

All things considered, government accountability and the rule of law require oversight bodies to assume a greater role in verifying the actual deletion of data. At present, there is often too much confusion and limited knowledge on the whereabouts of collected data that, technically and legally speaking, should no longer be in the possession of the intelligence community.

Idea: Deletion monitor

Modern intelligence laws and data protection regulations require intelligence services to record which data is deleted or destroyed as well as the point in time at which this occurs.[40] Logging data deletion is an essential part of any meaningful compliance effort. Data retention limits are relatively simple, binary rules: Data has either been deleted on time, or it has not. This simplicity makes these regulations very well-suited for automated oversight mechanisms.

[38] For a recent account of how legal provisions regarding data retention have been violated by the BND, see a leaked report by the German Federal Data Protection Authority: Meister, “Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by The Dozen,” 02 February 2016, https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/.

[39] Possible solutions to the deletion conundrum could be the introduction of purpose-oriented data retention approaches. For example, the USA Freedom Act requires regular re-examination of the necessity to keep data. Alternatively, data deletion could be based on a layered approach in which additional access restrictions would apply to the retrieval of older data. For example, datasets could be fully encrypted, and decryption after expiration of the retention period could then require prior authorization.

[40] For example, France has introduced legislation that stipulates that the destruction of collected intelligence, transcriptions, and extractions must be carried out by individually designated and authorized agents and recorded (Article L. 854-6. of French Law No. 2015-1556 on international surveillance).

If deletion activities are consistently recorded in well-structured log files, overseers can detect patterns and outliers over time. The Swedish oversight body reportedly runs statistical pattern analyses on the amount of deleted material.[41] This supports inspectors in more efficiently investing their resources towards suspicious patterns in data deletion.

Over a span of five years, for example, log files may reveal peaks in deletion activities on certain days that do not represent the official end of the retention period. If a warrant permits a certain dataset to be stored for six months, why has it been manually deleted after four months? Do the oversight body's announcements of pending spot checks spur "clean-ups" of databases? It is not feasible to review all deleted data – tracking deletion protocols over time may help oversight bodies to conduct more targeted investigations.

B4: Tracing the use of surveillance authorizations

Challenge

In some jurisdictions, an enormous number of surveillance warrants are produced every year.[42] Assessing the legality, necessity, and proportionality of government applications for surveillance measures represents a crucial accountability mechanism. Oversight bodies such as the Dutch TIB, the German G10 Commission, and the British IPCO authorize, approve, and re-assess significant amounts of applications for surveillance measures.

However, a comprehensive digital trail of the executive-oversight interactions in the authorization and, just as importantly, the implementation process is often lacking. How do oversight bodies keep abreast of the large volumes of applications when deciding on the necessity of new applications, for instance? In the absence of a system that provides an overview of existing authorizations and their implementation, overseers are ill-prepared to decide on new warrants.

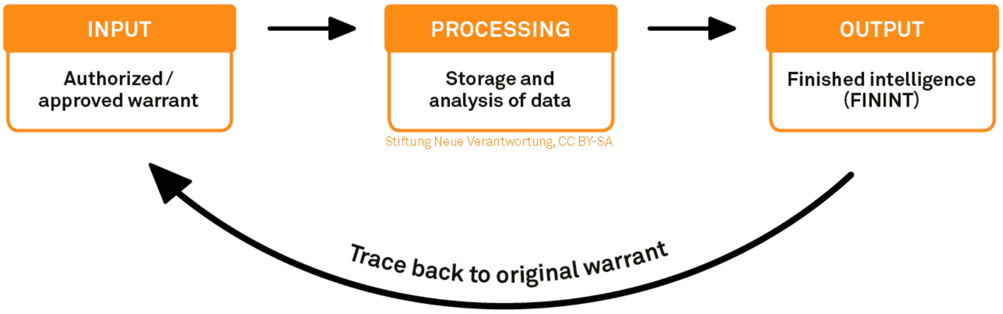
Moreover, there is another significant challenge inherent to the authorization process: Consider, for example, how some European intelligence laws require governments to provide a justification for each warrant application.

[41] Swedish State Inspection for Defense Intelligence Operations (SIUN), "Årsredovisning för 2017," 22 February 2018, Section 4.1, http://www.siun.se/dokument/Arsredovisning_2017.pdf.

[42] For example, the French oversight body CNCTR provided around 10,000 legal opinions on domestic interception warrants alone in 2018 (based on n. I of article L. 852-1 of the internal security code) and over 73,000 opinions across all intelligence collection methods, see: Commission national de contrôle des techniques de renseignement, "3. Rapport d'activité 2018," April 2019, p. 62, https://www.cnctr.fr/_downloads/NP_CNCTR_2019_rapport_annuel_2018.pdf.

Members of authorization bodies spoke to us about the problem of "boilerplate" text in application warrants, which comes about when justification arguments are merely cut and pasted, or are simply formulaic in content instead of comprising actual descriptions. They cautioned that the focus of reviews does not always have to lie on deviations or aberrant patterns. At least when it comes to warrant justification, reviewers would be well-advised to investigate excessive similarities between warrant justifications. We consider this to be another important oversight task that can be facilitated through automation.

Idea: Authorization tracker


INPUT
Authorized / approved warrant
PROCESSING
Storage and analysis of data
OUTPUT
Finished intelligence (FININT)
Trace back to original warrant

Stiftung Neue Verantwortung, CC BY-SA

Digital documentation of applications and decisions could support authorization bodies in their decision-making processes and help to detect applications that are either too broad in scope or too similar to existing measures (with unclear added value). Illustrations and statistics supplementing this digital documentation could assist reviewers in gaining a more accurate sense of the totality of surveillance measures currently in operation as well as the actual priorities of data collectors. There may be cases in which a government applies for a large number of measures and, upon their approval, decides to only act upon a few of them. For some surveillance powers, the French intelligence framework prescribes quotas that limit the number of parallel surveillance measures that may be authorized. Here, too, some kind of authorization tracker would appear to be necessary in order to verify that French intelligence services adhere to these quotas.

One mode of log file analysis would be to establish an "authorization-tracking system" that would enable all users (intelligence agencies and the reviewers) to create more granular propriety and efficacy benchmarks. Thoroughly tagging data origins, thus, allows oversight bodies to trace back a given dataset to specific accepted or modified warrants. Every warrant should be registered in the system along with its corresponding metadata/criteria, such as:

- Purpose/appropriation
- Third parties involved in the implementation
- Technical devices used for collection
- Duration of the warrant
- Storage period for the requested data
- Selectors or search terms used
- Types of data exploitation to be performed on the data
- Domestic and foreign security services with which the data may be shared

If the log files include the continuous tagging of the data origin, the intelligence agency and the oversight body can trace back finished intelligence products to warrants. Specific conditions that an authorizing body may have requested in approving a warrant can also constitute valuable imprints on collected data.

Empowering oversight bodies through authorization tracing

An authorization tracker could become an important compliance tool for independent authorization bodies. Presumably, a similar system already exists within intelligence agencies, which clearly also stand to benefit from this setup. Ideally, the warrant criteria would be automatically converted into the services' IT systems as part of their metadata management. Most IT systems depend on some form of standardized metadata catalogue, or on metadata dictionaries.[43] By design, warrant-based metadata should be a part of the intelligence agencies' operational data management and thereby of the audit logs.

For oversight purposes, the most relevant warrant-related metadata would probably include appropriation, purpose change, and retention period. The availability of this metadata could also be helpful in tracking the use and relevance of an authorized surveillance measure over time. Reviewers could measure which data sources have been most frequently used in intelligence analysis.

By juxtaposing (a) the entirety of data for which authorization was sought, (b) the collected data, and (c) the subset of examined data, overseers could

[43] For example, COBIT (Control Objectives for Information and Related Technologies) is an international standard for good practice in IT governance: https://en.wikipedia.org/wiki/COBIT.

assess the relevance, and by extension, the necessity of certain data collection measures with a greater degree of independence and with the help of reliable information. They might find that some warrants have never been implemented, or that, even though the data has been intercepted, it plays a negligible role in subsequent use.

We believe that these insights could help all oversight bodies. Those which have been explicitly tasked with assessing the efficacy of intelligence collection, such as the Belgian Vast Committee, might be particularly well-served by such a tool.

C. Smarter planning: Risk-based prioritization of oversight duties

Challenge

Intelligence oversight bodies need to perform a range of important and complex tasks with finite resources. In Germany and the United Kingdom, to name just two examples, oversight bodies inform the public of their annual agendas. This practice is laudable, as it provides additional transparency. However, when employees of the German parliamentary intelligence oversight body are assigned to report back to the oversight committee on specific themes and investigations,[44] it is unclear how these priorities are determined. Do these assignments cover the areas for which the greatest need for scrutiny is expected? If so, why is this the case? Is this due to a heightened risk of abuse or government malfeasance, or because of the need to establish oversight of hitherto-uncharted territory? At present, the prioritization criteria are not sufficiently clear. Many European oversight bodies can presumably improve when it comes to work prioritization. In other words, most countries can do a better job of pursuing the question of where to invest limited time and resources.

Instrument: Risk assessment[45]

The independent Danish intelligence oversight body TET has devised a systematic approach to sequencing and scheduling oversight activities that

[44] See, for example, "Unterrichtung durch das Parlamentarische Kontrollgremium (Progress Report of the German Parliamentary Intelligence Oversight Committee (PKGr)," 19 December 2013, p.6, https://dip21.bundestag.de/dip21/btd/18/002/1800217.pdf.

[45] Our description of the risk assessment approach is based on the TET's previous experience with the tool, which we learned of during the EION workshop on 10 May 2019 and in bilateral interviews. This method has been developed and adopted from similar models used in financial auditing.

merits further attention.[46] What type of engagement or task is most pressing, and why is it required? If controlling data processing by intelligence services should take precedence, which database run by which service should be selected for which kind of inspection? To arrive at answers to these and similar questions, the TET uses a risk assessment to prioritize and schedule its work. Overseers calculate risk scores for specific intelligence systems within their oversight mandate, which help them to determine the types and timing of inspections and other oversight tasks.

Before assessing the risk associated with a specific element of intelligence gathering – say, foreign intelligence collection by means of equipment interference – TET maps all of the data collection systems of which it is aware. Keeping track of the diverse storage locations, devices, IT systems, and software tools that the services use to collect, retain, and analyze data is crucial to meaningful risk assessment. This task poses a formidable challenge in and of itself. Moreover, the oversight body may be unaware of parts of the technical infrastructure or certain data collection methods. Accordingly, identifying and tracking previously unavowed components is an ongoing oversight process. Alternatively, as we will discuss in Chapter 3, the risk assessment may also be spearheaded by intelligence agencies, in which case oversight bodies would need to supervise the process.

As regards the current Danish practice, once TET has completed mapping all systems and devices of which it is aware and to which it has access, it applies a set of fixed categories to assess the risk associated with each system and its various sub-components. To illustrate this further, consider the seven categories that the Danish overseers typically use to conduct a risk assessment:

[46] The Danish Intelligence Oversight Board (TET) is an independent, external oversight body with full access to the operating systems used by the Danish intelligence agencies. The board comprises five members and is supported by a secretariat of nine persons. See: Danish Intelligence Oversight Board, "The Oversight Board," https://www.tet.dk/om-tilsynet/?lang=en.

Risk assessment category	Possible values
Area of oversight	data collection method A, B, C; data storage facilities D, E, F; data processing systems H, I, J, etc.
Specific sub-system	SIGINT systems A1, A2, A3, etc.
Legal basis	§ 4 of law XYZ
Assessment of materiality[47]	"High" = 2 "Medium" = 1 "Low" = 0 "Unknown" = 2 "N/A" = 0
Are legal compliance checks performed?[48]	"Yes, including relevant logging" = 0 "Yes, but no relevant logging" = 1 "No" = 3 "Unknown" = 3 "N/A" = 0
Are internal compliance checks performed?	"Yes, satisfactory" = 0 "Yes, but not satisfactory" = 1 "No" = 3 "Unknown" = 3 "N/A" = 0
Have the internal compliance checks revealed any errors?	"Yes, non-compliance with legislation" = 2 "Yes, minor errors" = 1 "No" = 0 "N/A" = 0
Has the oversight body previously conducted compliance checks of the system?	"Yes" = 0 "No" = 2 "N/A" = 0
Have the oversight body's previous compliance checks revealed any errors?	"Yes, non-compliance with legislation" = 2 "Yes, minor errors" = 1 "No" = 0 "N/A" = 0
Have the oversight body's compliance checks prompted any comments?[49]	"Yes, material comments" = 2 "Yes, minor comments" = 1 "No" = 0 "N/A" = 0

[47] Materiality refers to the essential characteristics of the oversight area, such as the nature and volume of data processed, the number of employees within the oversight area, and whether the area concerned is controlled by automated or human processes.

[48] For example, are there mandatory legal approvals of operational activities? If so, is this approval automated via "stop-and-go" processes with no possibility of circumvention? Is there a sufficient rights management regime in place? Is a sufficient regime in place for logging various activities within this area? What are the scope and nature of the training of relevant staff, and is this training ongoing?

[49] Comments are listed systematically for each system in order to ensure comparability over time. The factors that are not captured in the risk categories are also registered in the comments section; for example, assessment of the level of information security maintained by intelligence services, a general assessment of IT systems, and whether the initial mapping of operational systems must be revised or updated.

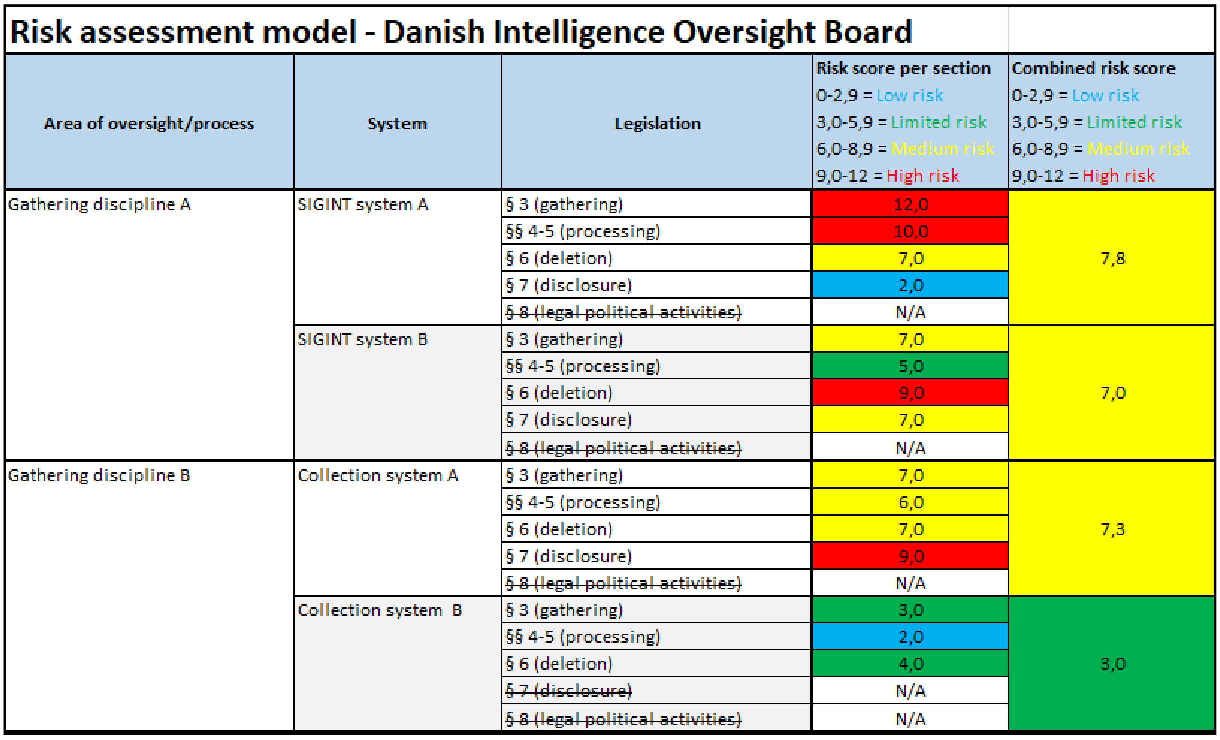
The risk scores are ranked in four risk categories:

Risk score **0-2.9**	**Low risk** of non-compliance with legislation
Risk score **3.0-5.9**	**Limited risk** of non-compliance with legislation
Risk score **6.0-8.9**	**Medium risk** of non-compliance with legislation
Risk score **9.0-12**	**High risk** of non-compliance with legislation

Each system (for example, a specific telephone metadata collection program) is subjected to the same rating method. The values for each category are assigned and listed in a spreadsheet. The final risk score is a numerical value between zero and twelve. This expresses the overall likelihood of a given statutory provision being violated within an oversight area. After this stage, a more detailed risk analysis is then conducted that takes into account additional aspects and more qualitative criteria, such as experiences gleaned from previous investigations. This step addresses the critical aspect of data incompleteness: At this point, the TET tries to evaluate if it has captured all relevant systems. If it suspects that the mapping is incomplete, it will conduct additional test inspections.[50]

The results serve as a basis for creating the annual oversight plan that sets the priorities for the oversight body and provides an overview of all controls and oversight processes. TET can therefore make better-informed decisions about which risks it is ready to accept and where to invest its limited oversight resources.

[50] For example, there might be legacy systems such as outdated computer systems (or software) that still store relevant data but are not yet on the oversight radar. Verifying this could be as simple as counting the number of servers in a room.



Risk assessment model - Danish Intelligence Oversight Board				
Area of oversight/process	System	Legislation	Risk score per section 0-2,9 = Low risk 3,0-5,9 = Limited risk 6,0-8,9 = Medium risk 9,0-12 = High risk	Combined risk score 0-2,9 = Low risk 3,0-5,9 = Limited risk 6,0-8,9 = Medium risk 9,0-12 = High risk
Gathering discipline A	SIGINT system A	§ 3 (gathering)	12,0	7,8
		§§ 4-5 (processing)	10,0	
		§ 6 (deletion)	7,0	
		§ 7 (disclosure)	2,0	
		~~§ 8 (legal political activities)~~	N/A	
	SIGINT system B	§ 3 (gathering)	7,0	7,0
		§§ 4-5 (processing)	5,0	
		§ 6 (deletion)	9,0	
		§ 7 (disclosure)	7,0	
		~~§ 8 (legal political activities)~~	N/A	
Gathering discipline B	Collection system A	§ 3 (gathering)	7,0	7,3
		§§ 4-5 (processing)	6,0	
		§ 6 (deletion)	7,0	
		§ 7 (disclosure)	9,0	
		~~§ 8 (legal political activities)~~	N/A	
	Collection system B	§ 3 (gathering)	3,0	3,0
		§§ 4-5 (processing)	2,0	
		§ 6 (deletion)	4,0	
		~~§ 7 (disclosure)~~	N/A	
		~~§ 8 (legal political activities)~~	N/A	

Extract of the spreadsheet used by TET to track individual risk scores of specific data collection systems and combined risk scores for intelligence gathering techniques.

Discussion

Based on its own risk-based capacity allocation, TET arrives at a more informed, verifiable, and reproducible decision about which intelligence activity or activities to review within a given timeframe. The Danish method provides added value for oversight professionals, intelligence agents, and the general public.

Firstly, it creates a structured overview of what could be overseen and what is actually overseen. This is an important achievement. Overseers (and, depending on the reporting, also the general public) obtain a far more granular sense of dark matter, gray zones, and white zones in terms of intelligence activity that has been actually reviewed in past as well as scheduled oversight missions.

Secondly, being forced to come up with risk scores for individual datasets or items in the intelligence community enables reviewers to gain far more detailed and hands-on knowledge over time about the breadth of the organizations that they oversee. In turn, they also become more aware of systems or processes with which they may not yet be familiar.

Thirdly, this approach helps to channel limited oversight resources more effectively. It can create greater transparency and open up resources for more targeted oversight.

Fourthly, it allows for routine and more specific feedback loops that help overseers to systematically assess the effectiveness of previous inspections and investigations. The risk assessment model is constantly being adjusted and updated to include new information. For example, overseers may have consistently selected foreign intelligence gathering through bulk collection of communications as a high-risk area that merits rigorous and continued scrutiny. Consequently, they may have conducted frequent, in-depth inspections on this matter. Over a longer period of time, this may have mitigated specific risks or cast them in a different light. Drawing on the results of their continuous engagement with the services allows overseers to update their risk score and fine-tune future investigations in light of information gleaned from feedback loops.

Fifthly, depending on how an oversight body reports on its oversight instruments and methods, the general public and intelligence services can have greater confidence in the maturity and suitability of these tools. Risk assessment allows oversight bodies to document and substantiate how and why they review certain elements of intelligence gathering. Intelligence services benefit from this increased professionalism because it means that they have to answer fewer random oversight requests. Meanwhile, the general public can better grasp which checks the oversight body is able to implement in practice.

All this being said, the Danish model also entails certain risks and disadvantages.

Firstly, the calculation of the risk score merely constitutes an approximation, and can be highly subjective depending on who executes the assessment, based on what knowledge. Clear documentation and peer reviews among risk auditors could help to mitigate this concern.

Secondly, the overall conclusion might be misleading or could create a false sense of completeness. Overseers using this method need to remain vigilant about blind spots. The risk score cannot be the only basis for decision-making regarding oversight priorities. It must be considered in context, enriched with additional information, and questioned by the overseers. For example, the category “Has the internal oversight revealed errors?” may be assigned the value 0 (for no revealed errors detected by internal review authorities).

There could be various reasons behind this; for instance, the internal oversight performed on a specific matter might have been dubious or perfunctory. Constant feedback and adjustment cycles therefore need to be incorporated into risk assessments so that they may serve as a solid, reliable basis for establishing work plans.

Thirdly, oversight bodies should reserve sufficient capacity for catching intelligence services and governments by surprise. As far as this is concerned the transparency of the risk assessment methodology might make oversight inspections overly predictable. Agencies could conceivably adapt in line with planned oversight investigations, which would thereby undermine these investigations' effectiveness. That being said, oversight bodies also depend on the cooperation of the intelligence agencies and the information that they share. Being open about oversight methods and preferences could foster honest dialogue. Bearing this in mind, oversight bodies should ideally aim for maintaining a good mix of foreseeable and unforeseeable oversight activities. A risk-based work plan could be combined with impromptu, unannounced audits and inspections to alleviate the risk associated with predictability.

To sum everything up, if done correctly, adopting the Danish method can certainly optimize oversight bodies' efficiency and knowledge base.

Empowering oversight bodies through strategic resource allocation

To put this approach into practice, oversight bodies must engage in continuous dialogue with the national intelligence community in order to be as accurate as possible when mapping data collection and data analysis systems. Intelligence agencies are likely to be simultaneously conducting their own risk assessments, and there is probably room for both: Oversight bodies can perform due diligence on the agencies' internal risk assessments. However, they should not limit their focus to passively reviewing intelligence agencies' risk assessment processes. There is a great deal to be gained by oversight bodies administering their own risk assessment, even if this is limited in scope The more accurate the initial mapping, the more effective the capacity allocation. Oversight bodies must make a collective internal effort to regularly use risk assessment as a tool and to implement regular feedback loops. At least one (ideally, several) dedicated persons with leadership responsibilities should be assigned to maintain the risk assessment system.

D. Regular knowledge exchange with private intermediaries

Challenge
Interactions between intelligence services, governments, and private carriers represent an important element of contemporary surveillance practice, yet they often remain a “gray box” for most oversight bodies. Agencies might install their own technical equipment and sometimes even rent their own separate rooms and facilities on the premises of an internet service provider. They may also compel carriers to do things that are of key interest to those reviewing the legality and propriety of intelligence governance. History has shown that oversight bodies must be aware of the potential for creative non-compliance and technical workarounds that – inadvertently or not – undermine legal requirements.

In the private sector, if an employee purchases goods beyond his or her actual authorization, this is referred to by auditors as “maverick buying.” For example, employees may buy products without involving the purchasing department, or may involve it too late in the process. These activities mostly fall below the threshold of illegal conduct, and there might be valid reasons for bypassing certain steps of a procurement process. However, if maverick buying occurs repeatedly or systematically across a given workforce, this can have severe ramifications for a company’s financial stability. This is why tracing maverick buying is a standard control activity in financial auditing.

Translated into the context of intelligence gathering, “maverick buying” could be unauthorized data collection from a telecommunication service provider or the incorrect installation of bearers at an interception point. How can oversight bodies spot and stop this type of “maverick collecting?”

Idea: Oversight-carrier dialogues
More systematic exchanges between oversight bodies and the communication service providers that route or store relevant data could help to address this challenge. Bilateral meetings would probably be the most efficient approach for large ISP’s that might receive dozens of security notifications for a range of different purposes. In addition to these meetings, a broader multilateral oversight-carrier forum could be established that also includes

smaller companies that only occasionally have to serve the government on the basis of a warrant.[51]

Discussion

Oversight officials need to be well-informed of how data collection is implemented in order to conduct proper assessments and inspections. This holds true for authorization bodies that approve warrants as well as review bodies that are charged with ex-post controls. Some oversight bodies have already established direct relationships with internet service providers (or postal operators, mobile network operators, communication service providers, etc.). These ties should be expanded to supplement the more technical oversight instruments.

Some intermediaries have noted ambiguities in the implementation of intelligence data collection. This demonstrates carriers' interest in addressing the risk of (creative) non-compliance at interception points. For instance, the internet exchange provider DE-CIX challenged the bulk interception warrants it received before the German federal administrative court.[52] The court ruled that the company's charges were formally inadmissible. However, the federal judges also stated that the warrants in question were leaving too much latitude for implementation.[53] The British Investigatory Powers Act (IP Act) also accounts for considerably broad discretion when it comes to implementing warrants: It stipulates that a warrant authorizes any conduct necessary to fulfill what is authorized or required by the warrant, including "the interception of communications not described in the warrant," or "obtaining secondary data from such communications."[54] The Norwegian EOS

[51] In the UK, the Technical Advisory Board (TAB) acts as a platform for exchange between agencies and companies. The board consists of six representatives of the communications industry (from O2, British Telecom, Vodafone, etc.), six representatives of the intercepting agencies, and a chairman who reports directly to the Home Secretary. See: https://www.gov.uk/government/organisations/technical-advisory-board. However, no (independent) oversight representatives are directly involved. In France, the regulatory authority for electronic communications (ARCPE) has the right to nominate one of the nine members of the CNCTR that has "substantial technical knowledge of electronic communication." This person is currently a representative of the telecommunication industry, which could also potentially promote the liaison between oversight and carriers.

[52] Bundesverwaltungsgericht (German Federal Administrative Court) press statement, "Klage der DE-CIX Management GmbH erfolglos" (Court rejects lawsuit filed by DE-CIX Management), 31 May 2018 (38/2018), https://www.bverwg.de/pm/2018/38.

[53] The oral hearing before the federal administrative court, for example, showed that the bulk warrant issued under the G10 law does not clearly determine which cables must be intercepted with which method. Instead, the BND sends separate emails to the carrier that specify the concrete ports to be intercepted and the devices used to divert the data stream.

[54] For targeted interception warrants, this is regulated in section 15(5) IP Act (see also Investigatory Powers Act 2016: Explanatory Notes, paragraph 67, http://www.legislation.gov.uk/ukpga/2016/25/section/67/enacted).

Committee mentions an inspection of Telia Norge in its last annual report.[55] Under British law, operators have an obligation to report errors, such as an erroneous interception or a data disclosure error, to IPCO and the agency concerned.[56]

A constructive dialogue between oversight bodies and industry would be highly beneficial to both sides: Oversight bodies would benefit from the information they would receive and would be able to track how data collection is implemented in practice. Carriers would enjoy the advantage of being able to clarify open legal questions or, in cases of doubt, be able to make use of a communication channel to report mistakes. Intelligence services would also stand to benefit if oversight bodies have a clearer picture of what is going on, as this would help to prevent misunderstandings regarding interpretations of the law.

[55] The EOS Committee's legal mandate includes a right to access information from public or private enterprises that assist intelligence and security services. Norwegian Parliamentary Oversight Committee, "EOS Committee Annual Report 2018," 27. March 2019, p. 39, https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf.

[56] Section 235 (6) of the IP Act states that "a public authority, telecommunications operator or postal operator must report to the Investigatory Powers Commissioner any relevant error (within the meaning given by section 231(9)) of which it is aware." A "relevant error" according to section 231 (9) means an error (a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and (b) of a description identified for this purpose in a code of practice under Schedule 7, (Investigatory Powers Act 2016, http://www.legislation.gov.uk/ukpga/2016/25/section/235/enacted).

3. An Agenda for Data-driven Oversight

The previous chapter introduced several tools that we believe merit further attention and which could form a key part of a more ambitious reform agenda for effective intelligence oversight. Few of the tools we discussed represent groundbreaking, previously unheard-of ideas – we mostly drew inspiration from existing practices in other policy fields, from the private sector, and from collaborative work processes used in the European Intelligence Oversight Network.[57]

Today, many oversight professionals seem to recognize the game-changing potential of data-driven oversight. Nevertheless, most European review bodies are still only scratching the surface in terms of the related possibilities. It is therefore highly laudable and timely that a group of six European oversight bodies has initiated "a new project that will focus on (1) the development of oversight and audit standards and (2) oversight innovation."[58]

As discussed above, there are still a range of potential pitfalls regarding both the design and the implementation of supervisory technology for intelligence oversight bodies. These ought to be addressed more thoroughly before recommendations are made for further advancing data-driven oversight.

3.1 Concerns and executive pushback

Executive privilege

Some argue that direct access and new ideas for supervisory technology are highly welcome if they are reserved for institutions within government. In other words only data protection and compliance units within intelligence agencies and under executive control should benefit from these tools. The concern underlying this position is that placing direct access to operational systems and powerful audit tools in the hands of independent oversight institutions, would infringe on executive privilege and must therefore be rejected.

Some of the ideas presented in this paper (such as data-sharing alerts and an authorization tracker) may seem incompatible with the notion that a government requires a core area of sole executive responsibility. This core area is especially needed, some argue, in the realm of security and intelligence, where

[57] European Intelligence Oversight Network, "Workshop on control tools," Stiftung Neue Verantwortung 10 May 2019, https://www.stiftung-nv.de/sites/default/files/agenda_second_eion_workshop_10052019.pdf.

[58] De Ridder, "A simple yet existential demand: Let oversight bodies work together," November 2019, https://aboutintel.eu/simple-oversight-demands/.

the stakes for public wellbeing are particularly high. Since independent oversight bodies are not obligated to provide security, they should also not be put in a position to become co-decision-makers.

To further illustrate this point, some refer to the notion of a *Parlamentsarmee* in German politics, whereby the Bundestag exerts direct budgetary *and* operational control over the deployment of Germany's armed forces. Critics invoke this example to argue that this type of approach is not how intelligence is meant to be governed. If the sovereign wanted to change this, it would first have to create a *Parlamentsnachrichtendienst* (i.e., an intelligence service steered by parliament). This would require fundamental changes to federal and state constitutions and, eventually, backing from the Federal Constitutional Court. The court may have placed limitations on the principle of executive privilege in its jurisprudence, but it has consistently underscored the need for space for deliberation on the part of the government.

This position on the role of executive privilege may vary across Europe due to manifold constitutional and socio-cultural differences. In Germany, there is certainly pushback against greater access and more audit tools for independent oversight institutions. However, this position seems to have less clout in other European nations, which have recently introduced substantial changes to their surveillance and intelligence laws. Consider Denmark's oversight body TET, for example. Despite its status as an independent oversight body, it enjoys direct access to log files and operational systems. It also has more modern audit tools at its disposal than German independent oversight bodies seem to do.[59]

[59] Variations in the institutional design and mandates for intelligence oversight bodies are due to a wide range of different factors. Some countries, such as the United Kingdom and Denmark, have granted their intelligence services far greater surveillance powers than others have. Lawmakers in these countries may have felt a greater need to put more powerful oversight structures in place. Elsewhere, oversight bodies may have received greater review mandates and access rights because their setup as independent expert bodies may allow for greater de facto "proximity to the executive." Interestingly, the latter reasoning does not seem to hold up, at least not for the Independent Committee and the G10 Commission in Germany. These bodies are subjected to greater access restrictions than the five European oversight institutions that have signed the Common Statement of Bern. See "Strengthening oversight of international data exchange between intelligence and security services", https://eos-utvalget.no/wp-content/uploads/2019/05/joint_statement_for_publication_20181114_final_endelig.pdf. Strictly speaking, the Independent Committee in Germany bears the characteristic traits of an administrative oversight body and is discussed as such in some literature and jurisprudence. See, for example, Graulich, "Reform des Gesetzes über den Bundesnachrichtendienst, https://kripoz.de/2017/01/15/reform-des-gesetzes-ueber-den-bundesnachrichtendienst-ausland-ausland-fernmeldeaufklaerung-und-internationale-datenkooperation/ See also: Bundesverfassungsgericht (German Federal Constitutional Court), "G 10-Kommission ist im Organstreitverfahren nicht parteifähig und scheitert daher mit dem Antrag auf Herausgabe der NSA-Sektorenliste" 14 October 2016 (72/2016), https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/ bvg16-072.html;jsessionid=7E07882B3FF5229720E12BEF0CB9498E.1_cid370.

Jeopardizing oversight independence?

There is also a risk of capture and of overly cozy relationships between the overseer and the overseen. Oversight bodies must take care to safeguard their autonomy and their role as an external corrective vis-à-vis intelligence agencies, which are significantly larger than they are. It is important for oversight bodies to retain an element of randomness and surprise and to conduct their investigations independently. They need to be aware that there is a line between cooperation and complicity that should not be crossed. Crossing this line – for instance, by becoming co-decision-makers – would potentially undermine oversight bodies' authority as independent reviewers. That is why overseers also have a vested interest in maintaining a certain distance from the agencies – this shields them from the risk of being made jointly responsible for flawed implementation or non-compliance with legal requirements. In other words, no oversight body should replace the roles of administrative leadership, general counsel, and internal compliance departments. That being said, oversight bodies also need to make sure that intelligence services design new systems in a way that render them overseeable. This will not be possible if oversight bodies shy away from engaging with intelligence officers during the planning stages because they fear that their hands will be tied later if scandals or irregularities arise. Experience gained from countries such as Denmark and the Netherlands shows that it is possible to advise the executive without compromising oversight independence.

Direct access – an information security nightmare?

Some caution that greater access comes with greater responsibilities. Understandably, IT security risks represent a widespread concern when it comes to giving overseers greater electronic access to operational systems and databases.[60] Administering an electronic oversight interface, some argue, would create an additional point of attack for foreign adversaries, cybercriminals, or saboteurs. At present, they warn, oversight bodies are simply nowhere near sufficiently equipped and trained to act as stewards of national security data – and, furthermore, some argue that too many investments would be needed to change this.

Yet, as practical experience in the Netherlands, Switzerland, and Norway has shown, oversight bodies and their infrastructures can be hardened against attacks and espionage. The oversight staff who directly use operational systems must be well-trained and follow the same security standards as intelli-

[60] The recently leaked security assessment of the Austrian domestic intelligence service BVT illustrates some common security concerns, such as the physical security of facilities and the risks of digital infiltration (through connected systems). See: Schmitt, "Alarm: Verfassungsschutz BVT steht total blamiert da," 11 November 2019, https://m.oe24.at/oesterreich/politik/Alarm-Verfassungsschutz-BVT-steht-total-blamiert-da/405465583.

gence officials do. When equally high levels of protections against breaches or data loss are in place, oversight professionals are no more vulnerable to hacking attacks than agents working in intelligence services. Given the enormous investments in surveillance and intelligence that governments have recently made, funds could feasibly be made available to bolster oversight information security, too.

Undue duplication

A more convincing argument, we believe, is advanced by those who caution against the risk of unnecessary duplicated audit tasks. Modern intelligence services and the executive bodies to whom they report are doubtlessly performing a wide range of audit tasks already. They, too, have an interest in effectiveness and legality. Accordingly, some argue that if independent oversight bodies were to design audit tools from scratch, this would not only take up too many of their scarce resources, but would also be a waste of time and money. Given that other institutions within the executive sphere must have compliance mechanisms in place, oversight bodies could help to improve them and perform due diligence reviews. Bearing this in mind, an oversight reform agenda should focus on the specific added value that external oversight entails and avoid duplication.

There is a lot to be said in defense of this argument. We also recognize that some of the tools we have proposed could be more readily implemented than others (see the section below). However, the underlying arguments in favor of implementing these tools are by and large consistent. Generally speaking, there needs to be closer cooperation between independent oversight bodies and the executive. An oversight reform agenda should certainly try to leverage synergies and use resources as best as possible. This requires governments to be prepared to embrace data-driven intelligence oversight. Then again, it would also be misguided to leave all types of advanced auditing solely to executive sphere. Oversight bodies should also be encouraged to probe and test the information that they receive with their own means – even doing so runs the risk of duplicating certain tasks – in order to maintain an element of surprise and avoid being captured. By merely engaging in reactive due diligence testing, overseers forego a great deal of practical knowledge that they would otherwise gain through more active probing.

Independent oversight bodies are not to be trusted

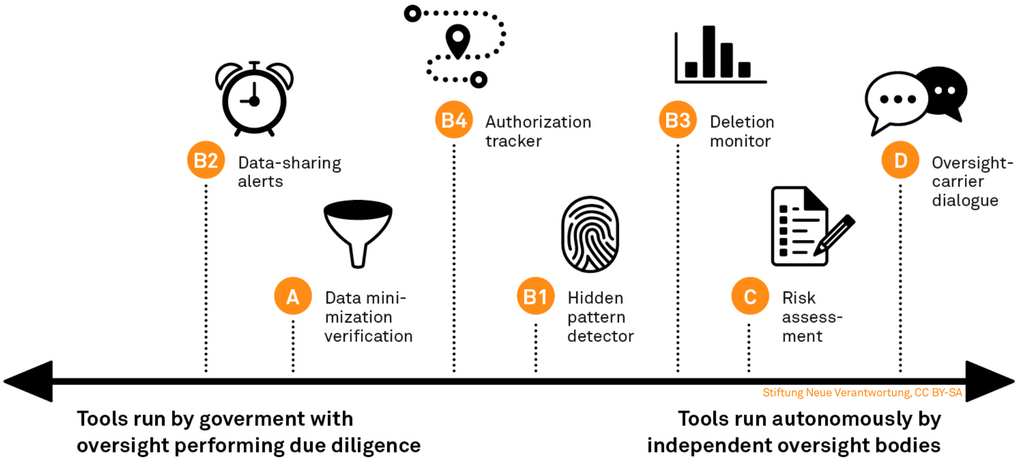
Some question the general integrity and reliability of oversight bodies. Providing oversight bodies with further access and tools, they argue, would only heighten the risk of sensitive material being leaked. We feel that this concern ought to be addressed carefully, on a case-by-case basis. Information leaks from parliamentary oversight bodies may have happened, but the evidence surrounding these cases often remains inconclusive. Moreover, executive bodies are also not immune to leaking information to the press for political gain. What is more, we are not aware of any cases in which sensitive information has been leaked by judicial or expert oversight bodies.

All of the concerns we have discussed thus far merit further scrutiny. We hope that we have persuasively demonstrated that the common arguments raised against tech-enabled oversight innovation can be countered, at least in part. When considering examples of existing practices across Europe, we see the practical feasibility and added value of the tools for independent oversight bodies.

We believe that the European countries that have granted their oversight bodies direct access to operational systems and which are pursuing data-driven review tools are on the right track and now need widespread support. What is more, in recognition of the widening gap between high-tech intelligence and low-tech oversight, we believe that ineffective oversight is just as pressing and important a concern: It poses grave risks to our democracies. Given the wide range of options for better oversight, it is difficult for us to imagine how any legal review mandate could continue to be justified without including direct access to the systems and databases used by intelligence services.

Who should wield the tools in the executive-oversight relationship?
The tools that we introduced in the previous chapter require different levels of cooperation and interconnectedness between oversight bodies and intelligence agencies. Put bluntly, some ideas can only be realized if the services provide the necessary infrastructure and data. Arguably, some tools should best be fully implemented by intelligence agencies, as they facilitate basic legal compliance that must be directly integrated in these agencies' operational processes and information infrastructure. After all, agencies have to ensure that they comply with the law. On the other hand, as argued above, independent oversight bodies must not risk being constrained by too close proximity to and dependency on intelligence agencies.

The diagram below shows how the tools we presented in Chapter 3 depend, in our view, on varying proximities to the executive when they are implemented in practice.


B2 Data-sharing alerts
A Data minimization verification
B4 Authorization tracker
B1 Hidden pattern detector
B3 Deletion monitor
C Risk assessment
D Oversight-carrier dialogue
Tools run by goverment with oversight performing due diligence
Tools run autonomously by independent oversight bodies
Stiftung Neue Verantwortung, CC BY-SA

We would suggest, for example, that the tools B2 (data-sharing alerts) and A (data minimization verification) are best implemented when oversight bodies run their own probes based on technical infrastructure that is run and maintained by intelligence agencies. Proper data minimization is a fundamental element of legal compliance and should first and foremost be the responsibility of the services. By contrast, we see that there is significantly more room for oversight bodies to autonomously implement risk assessments (D) or a deletion monitor (B3).

There will inevitably be some pushback from intelligence agencies and governments to some of the ideas presented here. In light of this, it might be a good idea to start by focusing on those elements which are most likely to garner support from the executive sphere, such as a deletion monitor. Proper deletion poses an enormous challenge; introducing a tool to tackle this would likely appeal to many stakeholders. Both governments and oversight bodies have a shared interest in effective deletion: Honoring retention limits for reasons of data protection and maintaining data security and data accuracy represent two sides of the same coin.

As far as other tools and concepts are concerned, recording log files and making them available (B) creates a win-win situation, which should be emphasized. If oversight bodies have access to robust audit trails (generated automatically by information systems), this would reduce the reporting costs for intelligence services. Enhancing the transparency reporting towards oversight bodies has positive side-effects, too. If overseers receive relevant logging data, as depicted in the risk assessment approach (D), they can focus their in-person inspections on other, more risky facets of intelligence activities. In turn, providing log files frees intelligence services from having to deal with undue oversight requests, thereby opening up resources and increasing effectiveness on behalf of both parts.

3.2 Prerequisites and policy recommendations

As is the case with international oversight cooperation, oversight innovation has been advocated for quite some time now, and some progress has certainly been made. However, whether it be due to a lack of political will or imagination, genuinely tech-enabled or even automated intelligence oversight has been inconclusively debated for too long.

We hope the following points and recommendations can encourage further debate that helps to bring about more tangible oversight innovations.

General recommendations

- **Oversight-by-design principle:** Intelligence services should ensure that their processes and information systems are designed to be overseen in an efficient manner. It is the responsibility of intelligence services to ensure overseeability across all phases of the intelligence process. This can be supported by establishing default early-stage consultations between the agencies and the oversight bodies whenever new data processing systems are created and ensuring that the agencies are bound to incorporate the input provided by oversight bodies at these consultations.[61]
- **Direct electronic access to operational systems:** It is difficult in this day and age to speak of effective intelligence oversight if oversight bodies lack comprehensive digital access to the data and operational systems used by intelligence services. As we have explained, effective oversight requires both direct access to information systems as well as the ability to pull datasets for in-depth offline analysis.
- **Evaluation of oversight capacity:** Oversight bodies should assess and highlight the gaps and deficits in their existing oversight mandates and bring these to the attention of policymakers and political leadership. This assessment makes it possible to draft context-specific strategies for data-driven intelligence innovation.

[61] French lawmakers have written this principle into law, demanding obligatory ex-ante opinions from the oversight body on data-tagging processes; see Wetzling and Vieth, 2018, p. 61f. Meanwhile, the German Federal Data Protection Authority is obligated to assess the legality and function of new intelligence databases for personal data before they are implemented; see § 14 (1) of the Act on the Federal Office for the Protection of the Constitution (Bundesverfassungsschutzgesetz), https://www.gesetze-im-internet.de/bverfschg/__14.html.

- **Make room for preparatory work:** Each of the tools we have presented presupposes a great deal of preparation and a willingness to experiment. For supervisory technology to work properly, it needs to be constantly tested and adjusted. This requires clarity in terms of goals and motives, human resources, knowledge of both the law and intelligence practices, and data analysis skills. Oversight bodies should hire one or two experienced data analysts in order to build up dedicated technical oversight capabilities.
- **Exchange with the private sector:** Oversight bodies can learn from the wealth of experience gleaned in other sectors, such as information security and financial supervision. They should look beyond national borders and existing partnerships to promote direct dialogue with the private sector and academia. Oversight bodies could benefit from examining existing solutions to some of the challenges related to developing additional auditing capacities. A wide range of off-the-shelf solutions exist that could, at the very least, be consulted to see what kind of monitoring is possible. Individuals who regularly advise government departments and security services should be invited to help modernize and improve accountability mechanisms.

Recommendations for improving data minimization verification

As discussed above, implementing filter technology will likely remain a matter of ensuring internal compliance within intelligence agencies. However, it is also a crucial role for oversight bodies to test filter results. Oversight bodies should perform randomized (yet regular) checks to test the accuracy of the data minimization technology that intelligence services use.

- **Due diligence reviews on stored data:** This requires unfettered access to the stored data that is kept after the minimization process. The results of these probes should be tracked over time so that oversight bodies can calculate a general error rate of an intelligence agency's filtering veracity. This would then enable the executive and lawmakers to make evidence-based decisions about the usefulness and feasibility of certain legal data protection categories.
- **Precise and realistic minimization rules:** Taking independent reviews and technical feasibility as a basis, lawmakers may introduce clear legal requirements indicating what filters need to achieve and whether an error rate is permissible.

Recommendations for making better use of log files
Both agencies and oversight bodies should embrace the mutual benefits of log file analysis as a means of semi-automated reporting. Logging obligations must be detailed in order to empower oversight. Given that log files are usually recorded for non-oversight related purposes, we emphasize the need to take oversight needs into consideration at an early stage when developing the technical setup for fulfilling logging requirements.

- **Introduce an obligation to maintain meaningful audit trails:** Log files and other relevant data should be collected and maintained in a way that caters to the needs of oversight bodies. This would include a legal obligation to record comprehensive log files that provide granular information, as well as a comprehensive data tagging system. These are already required by many data protection laws, and represent crucial prerequisites for the types of log file analysis described above.
- **Intelligence oversight hackathons:** Considering that oversight bodies are typically relatively small organizations with limited resources, in-house development may not always be feasible. Oversight bodies should therefore avoid reproducing existing systems and tools. That said, intelligence oversight entails unique requirements for technical solutions. Organizing intelligence oversight hackathons could attract external expertise and direct it towards the specific needs of intelligence oversight. In order to keep intelligence methods and data sources secret, a hackathon open to the public could be based on an abstract problem represented with synthetic data. There could also be an open call for ideas for pattern detection approaches.
- **Common reporting standards for transferred datasets:** Europe-wide, oversight bodies have to engage with national governments to establish common minimal reporting standards on what happens to shared data. If data can be shared with a foreign service, it must also be traceable for oversight.

- **Oversight cooperation on log file analysis tools:** Given the complexity involved in developing effective audit scripts, intelligence oversight bodies should exchange their experiences, identify best practices, and promote further capacity building as part of their international cooperation with other oversight bodies. To meet the challenges of their work, they should engage in joint assessment and mutual learning, performing experiments with statistical monitoring, data visualization, and pattern detection tools.

Recommendations for effective risk assessment

Taking a more systematic approach to prioritizing oversight activities is in the interest of all stakeholders. This model needs to be both transparent and adaptable.

- **Continuously mapping intelligence activity:** Based on an initial inventory of collection programs and databases, oversight bodies should ask the competent government departments or agencies whether this inventory is complete or if there are other elements that should be included. Repeating this process regularly allows to compare the results over time.
- **Public documentation:** To mitigate biases and reduce blind spots in risk assessments, provide clear documentation and manuals and establish routine peer reviews among risk auditors. Presenting the risk assessment approach in a transparent manner helps the general public to understand the value and impact of independent intelligence oversight.
- **Regularly evaluate the method:** Make room for structured reviews and adaptations to the risk assessment method.

Recommendations for oversight-carrier dialogues

Tech-enabled innovations should be accompanied by procedural safeguards. Mandatory error reporting and routine exchange formats complement data-driven tools.

- **Create an obligation to report errors to oversight:** To start substantial oversight-carrier exchanges, policymakers may introduce an error reporting obligation for providers that serve warrants. This commitment should ideally apply in the event of technical errors as well as cases of legal uncertainty and any suspected instances of creative non-compliance.
- **Transparency:** The frequency and form(s) of oversight-carrier engagement in practice should be included in public reporting in order to bolster the general public's confidence in the oversight body's work.

4. Conclusion

Moving forward, providing sporadic access to only a fraction of intelligence databases will hardly suffice for robust, modern oversight. Countries in which independent oversight bodies perform little more than compartmentalized and paper-based review tasks are oblivious to the rich potential that data-driven oversight has to offer. In the interest of democratic accountability and effective governance, change is urgently needed – and possible.

Given the sheer volume of data collected by intelligence agencies, effective oversight must be data-driven. To facilitate this, oversight bodies need to ensure that their specific needs are taken into account during the construction of operational systems. This alone will require preparatory work for years to come. However, in order to significantly advance the idea of *oversight intelligence*, it is important that reviewers embrace data-driven oversight tools – not as a replacement for their work, but as powerful supplementary tools that will allow them to work more efficiently. As is the case with automated medical diagnosis, data-driven tools will only succeed if they enhance the subjective judgement of the personnel using them. Obtaining user acceptance will require a genuine socialization process, which will also take time. For this process to succeed, additional expertise must be incorporated into oversight bodies, which will permit them to exercise greater autonomy from external consultants and intelligence services when necessary.

Increased expectations, responsibilities, and mandates pose a considerable problem: Oversight bodies obviously need more staff, resources, and expertise in order to be able to address many of the challenges we discussed in Chapter 2. These bodies must seize the opportunity to work in conjunction with intelligence services and policymakers and develop oversight innovation strategies that are suitable for specific national contexts. Naturally, best practices should be shared along the way, which is why we applaud the new project on oversight innovation and audit standards that six European oversight bodies have recently adopted.

In order for data-driven intelligence oversight to make headway, oversight bodies need more help and allies. Why should only the intelligence agencies, but not the oversight institutions enjoy access to sizable resources for research and development? Policymakers and Horizon 2020 planners in the European Commission should consider allocating dedicated R&D funding that explicitly focuses on supporting modern, data-driven oversight solutions.

Imagine what would happen if oversight bodies failed to innovate. National and international jurisprudence would continue to add to the list of serious oversight deficits. Further lawsuits will continue to test the robustness of oversight regimes. Legitimacy needs to be earned. A critical system update is now pending.

5. Annex

5.1 List of focus group participants and interviewees

We are very grateful for the help we received in writing this report and for the interest and time that a wide range of stakeholders have invested in our project. The following experts provided valuable input during the European Intelligence Oversight Network (EION) workshop held on 10 May 2019 or in bilateral interviews:

- Dr. Julia Thorsøe Ballaschk, Senior Advisor, Data Protection Unit, National Police, Denmark
- Wouter de Ridder, Secretary, Standing Intelligence Agencies Review Committee, Belgium
- Arild Færaas, Communications Adviser, EOS Committee secretariat, Norway
- Christian Flisek, Deputy Member, G10 Commission, Germany
- Dr. Luka Glušac, Office of the Serbian Ombudsman, Serbia
- Dr. Emil Bock Greve, Head of Secretariat, Intelligence Oversight Board, Denmark
- Giles Herdale, Associate Fellow, Royal United Services Institute (RUSI), United Kingdom
- Dr. Bertold Huber, Deputy Chair, G10 Commission, Germany
- Rune Odgaard Jensen, Intelligence Oversight Board, Denmark
- Thomas Kugelmeier, Office of the Federal Commissioner for Data Protection and Freedom of Information, Germany
- Klaus Landefeld, Director Infrastructure & Networks at eco – Association of the Internet Industry and Supervisory Board member of DE-CIX International, Germany
- Stuart Macleod, Inspector, Investigatory Powers Commissioner's Office, United Kingdom
- Charles Miller, Inspector, Investigatory Powers Commissioner's Office, United Kingdom
- Adam Steen Petersen, Data Protection Unit, National Police, Denmark
- Dr. Jörg Pohle, Head of Research Program "Data, Actors, Infrastructures," Alexander von Humboldt Institute for Internet and Society, Germany
- Kjetil Otter Olsen, Technical Director, EOS Committee secretariat, Norway

- Sir Bernard Silverman FRS, Chair of the Technology Advisory Panel, Investigatory Powers Commissioner's Office (IPCO), United Kingdom
- Dr. Sabine Sosna, Office of the Federal Commissioner for Data Protection and Freedom of Information, Germany
- Dr. Félix Tréguer, Researcher, Sciences Po Center for International Studies and Founding Member of La Quadrature du Net, France
- Dominic Volken, Deputy Head, Independent Oversight Authority for Intelligence Activities, Switzerland

5.2 References

Aaronson, Trevor. 2019. “A Declassified Court Ruling Shows How The FBI Abused NSA Mass Surveillance Data.” The Intercept. October 10, 2019. https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/.

Babuta, Alexander. 2019. “A New Generation of Intelligence: National Security and Surveillance in the Age of AI.” RUSI.Org. February 19, 2019. https://rusi.org/commentary/new-generation-intelligence-national-security-and-surveillance-age-ai.

Becker, Rainer, and Christian Schulz. 2016. “Wieviel Geheimdienst Braucht Deutschland?” November 16, 2016. https://www.swr.de/film/bnd-schattenwelt-geheimdienst-doku-nachrichtendienst-swr/-/id=5791128/did=17666664/nid=5791128/1o343xj/index.html.

Bundestag (Federal German Parliament). 2013. “Bericht Über Die Kontrolltätigkeit (Progress Report of the Parliamentary Oversight Committee (PKGr) Nr. 18/217).” 18/217. Berlin. https://dip21.bundestag.de/dip21/btd/18/002/1800217.pdf.

Bundesverfassungsgericht (German Federal Constitutional Court). “G 10-Kommission Ist Im Organstreitverfahren Nicht Parteifähig Und Scheitert Daher Mit Dem Antrag Auf Herausgabe Der NSA-Selektorenlisten (Federal Constitutional Court Rejects G10 Commissions Claim of Access to NSA’s Selectors),” October 14, 2016. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2016/bvg16-072.html;jsessionid=7E07882B3FF5229720E12BEF0CB9498E.1_cid370.

Bundesverwaltungsgericht (German Federal Administrative Court). 2018. “Klage Der DE-CIX Management GmbH Erfolglos (Court Rejects Lawsuit Filed by DE-CIX Management).” May 31, 2018. https://www.bverwg.de/pm/2018/38.

Cavan, Jo, and Paul Killworth. 2019. “GCHQ Embraces AI, but Not as a Blackbox.” *About:Intel* (blog). October 8, 2019. https://aboutintel.eu/author/jo-cavan-paul-killworth/.

Commission national de contrôle des techniques de renseignement. 2019. “3. Rapport d’activité 2018.” https://www.cnctr.fr/_downloads/NP_CNCTR_2019_rapport_annuel_2018.pdf.

Corfield, Gareth. 2019. “London Cop Illegally Used Police Database to Monitor Investigation into Himself.” The Register. July 11, 2019. https://www.theregister.co.uk/2019/07/11/met_police_sgt_pleads_guilty_computer_misuse_crimes/.

Dutch Review Committee on the Intelligence and Security Services (CTIVD). 2019a. “Annual Report CTIVD 2018.” https://english.ctivd.nl/binaries/ctivd-eng/documents/annual-reports/2019/06/20/index/CTIVD+annual+report+2018.pdf.

———. 2019b. “Progress Report.” CTIVD nr. 63. https://www.ctivd.nl/documenten/rapporten/2019/09/03/index.

———. 2018. “Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD (CTIVD Review Report No. 56).” https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2018/04/24/index/CTIVD+Review+report+NO56.pdf.

European Court of Human Rights. 2018. “Case of Big Brother Watch and Others v. The United Kingdom.” http://hudoc.echr.coe.int/eng?i=001-186048.

Federal Commissioner for Data Protection and Freedom of Information. 2019. “27. Tätigkeitsbericht (27th Progress Report on Data Protection and Freedom of Information).” https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/27TB_17_18.pdf?__blob=publicationFile&v=4.

Foreign Intelligence Surveillance Court. 2018. “FISC Opinion Regarding the Section 702.” Washington D.C. https://www.documentcloud.org/documents/6464604-2018-FISC-Ruling-Shows-How-FBI-Abused-NSA-Mass.html.

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

Golla, Sebastian. 2019. “Neugier Und Datenkriminalität.” Legal Tribune Online. August 16, 2019. https://www.lto.de/recht/hintergruende/h/polizei-datenbanken-missbrauch-datenkriminalitaet-abfragen-daten-schutz/.

Government Communications Headquarter. 2019. “Investigatory Powers Act.” March 19, 2019. https://www.gchq.gov.uk/information/investigatory-powers-act.

Graulich, Kurt. 2017. “Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und Internationale Datenkooperation (The legal reform of foreign-foreign surveillance by the German Federal Intelligence Service regarding international data cooperation),” Kriminalpolitische Zeitschrift (KriPoZ), no. 1/2017: 43–52.

Koenig-Archibugi, Mathias. 2004. “International Governance as New Raison d’état? The Case of the EU Common Foreign and Security Policy,” European Journal of International Relations, no. 10 (2). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.893.1837&rep=rep1&type=pdf.

Lohse, Eckart. 2019. “Kanzleramt Übt Heftige Kritik an BND (German Chancellery Heavily Criticizes BND),” April 23, 2019. https://www.faz.net/aktuell/politik/inland/kanzleramt-uebt-heftige-kritik-an-bnd-13555622.html.

Meister, Andre. 2016. “Secret Report: German Federal Intelligence Service BND Violates Laws And Constitution By The Dozen.” Netzpolitik.Org. February 2, 2016. https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/.

Norwegian Parliamentary Oversight Committee. 2019. “EOS Committee Annual Report 2018.” Annual Report. EOS Committee. https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf.

———. 2018. “Strengthening oversight of international data exchange between intelligence and security services,” October 22, 2018, https://eos-utvalget.no/wp-content/uploads/2019/05/joint_statement_for_publication_20181114_final_endelig-2.pdf.

Perraudin, Frances. 2019. “Mordaunt Pledges to Review Internal MoD Torture Guidance,” May 20, 2019. https://www.theguardian.com/uk-news/2019/may/20/mordaunt-pledges-to-review-internal-mod-torture-guidance.

Ridder, Wouter de. 2019. “A Simple yet Existential Demand: Let Oversight Bodies Work Together.” About:Intel. November 2019. https://aboutintel.eu/simple-oversight-demands/.

Ryngaert, Cedric, and Nico van Eijk. 2019. “International Cooperation by (European) Security and Intelligence Services: Reviewing the Creation of a Joint Database in Light of Data Protection Guarantees,” International Data Privacy Law, no. 9 (1) (April). https://academic.oup.com/idpl/article/9/1/61/5427456.

Schmitt, Richard. 2019. “Alarm: Verfassungsschutz BVT Steht Total Blamiert Da (Alarming: Austria’s Intelligence Service BVT Disgraces Itself to European Partners),” November 11, 2019. https://www.oe24.at/oesterreich/politik/Alarm-Verfassungsschutz-BVT-steht-total-blamiert-da/405465583.

Smith, Graham. 2019. “What Will Be in Investigatory Powers Act Version 1.2?” October 30, 2019. https://www.cyberleagle.com/2018/10/what-will-be-in-investigatory-powers.html.

Swire, Peter, Jesse Woo, and Deven R. Desai. 2019. “The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance,” A Hoover Institution Essay, January 19, 2019.

Venice Commission. 2015. “Report on the Democratic Oversight of Signals Intelligence Agencies.” CDL - AD (2015) 011. Adopted by the Venice Commission at its 102nd Plenary Session. Strasbourg. http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

Wetzling, Thorsten. 2017. “Options for More Effective Intelligence Oversight.” *Discussion Paper.* https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

Wetzling, Thorsten, and Kilian Vieth. 2018. *Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations*. Schriften Zur Demokratie 50. Berlin: Heinrich-Böll-Stiftung. https://www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and.

About the Stiftung Neue Verantwortung

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 organization 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.

About the Authors

Kilian Vieth

Kilian Vieth manages SNV's work on digital rights and surveillance. He is the project manager for the European Intelligence Oversight Network (EION), which provides intelligence oversight officials and other experts a space for regular and structured exchange. As a member of the GUARDINT research project, he studies the potentials and limits of overseeing surveillance and works on the development of an intelligence oversight index and a transnational surveillance law database.

kvieth@stiftung-nv.de
+49 (0)30 81 45 03 78 88
@newsvieth

Dr. Thorsten Wetzling

Thorsten Wetzling heads the SNV's research on surveillance and democratic governance. He directs the European Intelligence Oversight Network (EION) and is a Principal Investigator in the new collaborative research project GUARDINT designed to address and to redress the gap between increasingly transnational surveillance practices and still largely national accountability mechanisms. Since 2019, Thorsten helped design and implement aboutintel.eu – a new multi-stakeholder platform for a European conversation on all things intelligence.

twetzling@stiftung-nv.de
+49 (0)30 81 45 03 78 93
@twetzling

Imprint

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Editing:
Martha Turewicz

Graphic Design:
Anne-Sophie Stelke
www.annesophiestelke.com