PRIVACY AND CYBER SECURITY ON THE BOOKS AND ON THE GROUND

Ingolf Pernice, Jörg Pohle (Eds.)

ALEXANDER VON HUMBOLDT INSTITUTE FOR INTERNET AND SOCIETY
BERLIN, GERMANY

CONTENTS

LOOKING FOR COMMON GROUND IN A GLOBAL PERSPECTIVE

THE REGULATORS' TOOL BOX

Better intelligence oversight through technology? New perspectives on an old problem.

THORSTEN WETZLING

INTRODUCTION

Modern security and intelligence services use a range of digital powers to pursue their important mandates. Some of these powers, such as the electronic surveillance of communication data or computer network exploitations, can be highly invasive and may substantially interfere with human rights. Effective checks and balances are therefore imperative in order to review the legality and propriety of the use of such powers. Independent review bodies have to be able to challenge and, where necessary, penalise their abuse.

Despite recent reforms to further professionalise national intelligence oversight frameworks in Europe and North America, effective intelligence oversight remains an ambitious, unattained and vague benchmark on both sides of the Atlantic. Oversight dynamics on the ground continue to be marred by a range of problems, including ineffective control mechanisms, regulatory capture, a lack of technological knowledge and insufficient motivation to engage persistently in proactive and unglamorous investigative review work. In addition, one can point to no-go-zones and accountability gaps in conjunction with international intelligence cooperation and the outsourcing of intelligence functions to private contractors.

It is against this backdrop that the search for oversight innovation remains important. It should not be driven by government and legislators alone. Considering how the pace of technological innovation challenges core concepts of intelligence law and oversight practice, a broader set of perspectives is now needed to identify and promote viable options for positive change.

Drawing on insights from an ongoing transatlantic project,[1] this text first elaborates on a few current challenges to illustrate the need for oversight innovation. Next, it points to aspects where a more systematic and creative use of technology might help oversight bodies to better address known deficits. It then sketches out a few options that may make a difference if put into practice. Whether and how this might work and whether it might encounter new problems requires further analysis and actual feedback from intelligence governance practitioners across different branches of government. This dialogue can

[1] For more information on the project, see https://www.stiftung-nv.de/en/project/international-cyber-security-policy#drei.

obviously not be taken for granted and requires a carefully calibrated strategy of its own.[2] Only with sufficient support from oversight practitioners can any of the ideas be turned into a viable technology-driven reform agenda.

ON THE NEED FOR OVERSIGHT INNOVATION AND A PATH TOWARDS IT

As the conference title rightly conveys, significant differences exist in both Europe and the U.S. as regards privacy and cybersecurity on the books and on the ground. This is certainly true also in the field of intelligence governance. There is no shortage of guiding principles and international calls for effective democratic control and independent oversight. For a recent example, consider the UN resolution on the right to privacy in the digital age: It 'calls upon all States to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data'.[3] While it is important to regularly and visibly remind governments of the need to allow independent review of their invasive surveillance practices, the UN's call for independent, competent, informed, agile and resourceful oversight bodies has remained relatively inconclusive and as such is very convenient for Member States to support. By contrast, it is a much harder task to establish robust oversight in actual practice and to agree internationally on best practices. Recently, the international community rebuffed the UN Special Rapporteur on the Right to Privacy's attempt to establish international standards on government surveillance and human rights safeguards.[4]

Seeing intelligence oversight thus as an ambitious, unattained and vague benchmark, the transatlantic project mentioned above considers oversight innovation as work in progress not just for legislators and government. It seeks to bring multistakeholder expertise together in an attempt to develop pragmatic and innovative solutions to current oversight challenges. This includes regular transatlantic workshops with former oversight body representatives, telecommunication providers, academics and civil society representatives. Using collaborative work methods in carefully scripted workshops, it offers a chance to better understand the underlying factors for good or bad practices and the potential for oversight innovation, regardless of the constitutional and political differences among countries.

[2] One such strategy, for example, is the European Intelligence Oversight Network. More information available at https://www.stiftung-nv.de/sites/default/files/eion_project_strategy_brief_0.pdf.

[3] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1.

[4] See https://www.ip-watch.org/2018/03/07/un-rapporteur-privacy-rebuffed-surveillance-oversight-negotiations/.

As a first step, the project identified examples of post-reform oversight deficits in Europe and in the U.S. Next, the workshop participants clustered and weighed a wide range of challenges according to different parameters such as criticality. Among those challenges were secrecy and the flaccidity of some oversight members. While these are critical and unresolved aspects, the group then focused on challenges that concern access to information. More specifically, the question arose of how technology might be used to allow for a less credulous and more adversarial oversight game in the future.

CURRENT AND FUTURE CHALLENGES

In December 2016, the Bundestag passed the most comprehensive reform of intelligence legislation in over two decades. Yet many known deficits have remained in place.[5] For example, at present, there is hardly room, let alone sufficient resources for a rigorous monitoring of data processing through the quasi-judicial G10-Commission. Moreover, there is hardly any digital documentation that would allow individual members of the G10-Commission to review the way in which their authorisation decisions have been implemented.

By European comparison, both the Netherlands and the United Kingdom have experienced granular debates about the standards in law and in practice concerning the authorisation of bulk surveillance. Irrespective of what one makes of the authorisation standards that these countries have adopted, the equally —if not more— important safeguards concerning data handling by intelligence services remain insufficiently legislated across Europe.[6] How the services treat data once they have acquired it and whether their data minimisation and data deletion procedures are adequate and independently verified is a matter that requires further attention and scrutiny.

Another challenge lies in what may be called 'non-intelligence intelligence'. This includes the re-use of commercial databases for intelligence purposes. More generally, as more and more software seems to be converging across different sectors, it becomes more difficult to distinguish clearly between data-sensitive intelligence and police and military operations. By contrast, the remit of intelligence oversight bodies remains strictly tied to intelligence service activity. It is time to ask more critically what it is that oversight bodies should be reviewing and whether some of the distinctions used in national security legislation and parliament are outdated.

[5] For a more detailed analysis of the reform, see: T. Wetzling, Germany's intelligence reform: More surveillance, modest restraints and inefficient controls (Berlin: Stiftung Neue Verantwortung, 2017). Available online: https://www.stiftung-nv.de/de/publikation/germanys-intelligence-reform.

[6] For a recent review, see Q. Eijkman, N. van Eijk and R. van Schaik, 'Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?' (2018). Available online: https://www.ivir.nl/publicaties/download/Wiv_2017.pdf.

Another challenge has to do with the fact that counter-terrorism and cyber security accrue different data needs. In 2015, the Bundestag added a clause to a central intelligence law that allowed non-targeted bulk surveillance to prevent hostile cyber operations against critical infrastructures. While counter-terrorism intelligence data needs were often portrayed as being kept within limits, it appears that the vigilant protection against cyber threats requires a different monitoring of electronic signals. How an individual oversight body can ensure that the interception of communications data is proportionate, given such different data needs, and how it can identify abuse has not become easier to understand.

Another aspect that can be raised to highlight current oversight problems is the insufficient regard for the summary effect of existing surveillance activities when authorising new warrants. In 2005, the German Constitutional Court coined the term 'Überwachungsgesamtrechnung'. Basically, the Court announced that individual authorisation decisions rarely take into account the total sum of existing surveillance measures. It would indeed be beneficial to future intelligence governance if the authorisation of warrants had to be made in full cognisance of other active measures. This idea has not resonated enough among security circles. At the time that the G10 Commission or the FISA Court is being asked to authorise an individual surveillance warrant, do they arrive at that decision with sufficient knowledge of other existing surveillance measures that are being run for the same purpose? At present, the reviewers will only assess the merits of a warrant on an individual basis. Here it might be possible to visualise some form of surveillance warrant that would in future help overseers to determine the need for more surveillance.

POTENTIAL TECHNOLOGICAL SOLUTIONS?

These are only some of the challenges that have come up in the ongoing project work.[7] As concerns potential legislative or technological solutions to better address some of these challenges, we have begun to search for ways in which judicial overseers can be empowered with readily accessible information on the totality of existing surveillance measures at the time when they are deciding whether or not to authorise new warrants. Here one needs also to discuss whether this should only concern the information on existing measures by national security services or whether the growing density of existing European counter-terrorism databases can also be added to a potential visualisation tool.[8]

[7] For a more comprehensive overview, see: T. Wetzling, Options for more effective intelligence oversight. (Berlin: Stiftung Neue Verantwortung, 2017).

[8] H. Busch and M. Monroy, 'Counter-terrorism and the inflation of EU databases' (2017). Available online at https://digit.site36.net/2017/05/23/counter-terrorism-and-the-inflation-of-eu-databases/.

Another idea by a group member was to establish authorised third-party time-stamping services for warrants and the publication of cryptographic fingerprints for such information. This would address some of the current deficits in the ex-post control of individual surveillance measures because it would allow reviewers to link the activities to an existing warrant and see whether the activities have been compliant with the warrant or not. Any deviation of data acquisition (e.g. a different telecommunication net or a longer duration) could thus be detected without revealing critical information.

Another idea that has come up is to find a way to better quantify intrusion. We need new instruments to unpack and evaluate the privacy intrusion of data processing tools. The majority of laws regulating the use of SIGINT techniques are predicated on a two-stage authorisation framework —an initial sign-off for large-scale access, and a second authorisation process when an intelligence officer wishes to view or analyse the collected information (usually only required if viewing a particular citizen's material). This authorisation model often fails to take into account interference with rights in between these two stages caused by the use of data processing and analytical techniques. These include the use of speaker recognition, emotion detection, language identification, content summarisation, link analysis as well as automatic enrichment of material, and the processing of material creating query-focused datasets. As these techniques become more widespread, a common understanding of how and where privacy intrusion occurs and is impacted will be essential to ensure that a rights-compliant and appropriate framework exists (both in internal agency policy and in statute). Opportunities to attempt to quantify this intrusion could also provide critical data to overseers, and methods to model various intrusion points could help provide some means of measuring exactly to what extent an individual privacy is being interfered with.

Another way forward would be the installation and independent certification of oversight interfaces. There are backend interfaces for the law enforcement community, but there is no such direct access for oversight bodies. Some European countries such as Norway or the Netherlands have given independent oversight bodies almost exclusive access to the online directories of intelligence service databases. One could think about requiring manufacturers to build in standardised, independently controlled interfaces at interception point (i.e. at an internet hub such as the Frankfurt-based DE-CIX) to better comprehend the acquisition practice of the intelligence services and to evaluate the practical necessity of the enormous amount of data held.

Also, as regards the data minimisation process, some countries have publicly revealed their elaborate filter systems that are being put in place to adhere to different data protection standards for national and non-national data. Provided an independent verification of the filtering process could be achieved, one could run so-called 'sock puppet audits' on the system. It would allow the review body to test the performance of the filtering process by entering false data into the system and see if the filters were

able to identify such an irregularity. This ties in with questions regarding the design, performance and transparency of control algorithms.

CONCLUSION

What can make the threat of defunct intelligence oversight loom less large? To alleviate existing capacity problems, it is time to think more creatively about how technology can be designed and deployed to better serve the overseers' needs. As intelligence and security services are pioneering digital tools for their work, it might seem as too obvious a solution to also apply advanced technological tools from the overseers' end. However, this is at present generally not happening, even though some oversight bodies might be currently experimenting with different types of solution.[9] More research and open dialogues are clearly necessary so that viable technological solutions can be identified and combined with better training of the overseers in combination with properly staffed and robust secretariats with legal, political and technical expertise.

[9] K. Otter Olsen, 'De hemmelige tjenestenes tekniske kapasiteter – kontrollutfordringer' (Annual EOS-conference, Oslo, 5 April 2017). See also M. R. Koot, 'Dutch Review Committee on the Intelligence & Security Services (CTIVD) to (self-)assess effectiveness of lawfulness oversight re: large-scale & data-intensive spying' (2017). Available online at https://blog.cyberwar.nl/2017/04/dutch-review-committee-on-the-intelligence-security-services-ctivd-to-self-assess-effectiveness-of-lawfulness-oversight-re-large-scale-data-intensive-a/.