November 2017 · Thorsten Wetzling

Options for more Effective Intelligence Oversight

Discussion Paper

Stiftung
Neue
Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Despite new guiding principles, international reports and comprehensive legislative reforms, effective intelligence oversight remains an ambitious and unattained benchmark. Democratic control bodies urgently need better review mechanisms and technological knowledge to understand, monitor and challenge the use of highly invasive and constantly evolving surveillance powers by national intelligence services.

Oversight is not a finished product. Rather it is constant work in progress. Much work can be done to significantly improve its effectiveness. The Stiftung Neue Verantwortung founded a multi-sectoral, transatlantic forum to contribute to this quest for better practice. This paper initiates the forum by introducing perspectives on pressing current challenges and, more importantly, some technological and regulatory options for positive change.

A thorough analysis of post-Snowden oversight dynamics in many established democracies reveals striking discrepancies between the practice on the books and on the ground. For example, judicial control bodies in many countries may have improved their position regarding the authorization of interceptions warrants. Yet, the even more important implementation of surveillance warrants remains far less often subject to rigorous review, let alone public reporting. Did the services collect only what was stated in the warrants and did they delete the data as required by law? This is hard to fathom in the absence of a digital trail documenting the implementation of surveillance measures. Similarly, the review of surveillance measures become far less meaningful when they are being conducted with insufficient knowledge of the search terms. Overseers still have to trust the services with regard to the performance of the filters used for data minimization. In the absence of independent verification and control audits, the accuracy of data triage by the services remains unconfirmed.

Due to the rights infringing and secret nature of electronic surveillance, these and other oversight deficits discussed in the paper are highly problematic. They ought to be fixed to guarantee more effective checks and balances. It is with this aim in in mind that the second part of the paper points to technological and regulatory tools that oversight bodies may promote to better ascertain the legality and efficiency of modern electronic surveillance. This includes oversight interfaces in communication backend systems, sock puppet audits to independently verify the performance of surveillance software and the publication of cryptographic fingerprints of interceptions orders. As surveillance software and hardware converge across different branches of government, intelligence oversight bodies should also be empowered to review non-intelligence intelligence such as the enrichment of commercial data for intelligence purposes and the communication surveillance without probable cause by military and police forces.

Recent Perspectives

“The Bill retains 20th century safeguards. It emphasises the classic safeguards of authorisation and assessment prior to the use of powers. The technological developments primarily require a strengthening of the safeguards in the data processing process where the infringements actually take place.”

CTIVD on the Dutch Intelligence and Security Act

“The services ought to guarantee that automated data processing does what it is expected to do and the oversight body must be able to ascertain this.”

CTIVD on the Dutch Intelligence and Security Act

“The era of big data requires big compliance, and a fundamental part of big compliance is the reconciliation of the written rules with a very real set of technologies”

John DeLong, Former Director of Compliance, NSA

“Judge Hogan orders the government to report to FISC every compliance incident that relates to the operation of either the targeting procedures or the minimization procedures it has just approved”

Lawfare Summary of 18 FISA Court Opinions on Section 702

“The Agency will stop the practice to reduce the chance that it would acquire communications of U.S. persons or others who are not in direct contact with a foreign intelligence target.”

NSA, Public Statement regarding “About Collection”, 2017

“We need to more deeply grapple with how to extend the underlying structural principles of transparency, some form of public input, and adversarial judicial review to the intelligence space.”

Daphne Renan in: Global Intelligence Oversight
(eds. Zach Goldman/Samuel Rascoff)

Content

I. Introduction[1]

Modern security and intelligence services use a range of digital powers to pursue their important mandates. Electronic surveillance and hacking are only two such powers. They are highly invasive and rights infringing. Effective checks and balances are therefore imperative to monitor, to challenge and to sanction the abuse of these powers.

There is no shortage of guiding principles, international reports and legislative reforms promoting effective intelligence oversight. Independent, competent, informed, agile and resourceful oversight bodies are often called for. This is an easy call to make and a much harder fact to establish in actual practice. Despite recent measures to further professionalize and democratize national oversight frameworks in Europe and North America, oversight dynamics on the ground continue to be marred by various problems. Among those are ineffective control mechanisms, regulatory capture, a lack of technological knowledge and an insufficient motivation to engage persistently in proactive and unglamorous investigative oversight work. In addition, one can point to no-go-zones and accountability gaps in conjunction with international intelligence cooperation or intelligence activities by agencies and contractors that are not subject to the same oversight regime.

A lack of objective performance indicators and government secrecy make it also difficult to assess, let alone compare, oversight performances. Individual political systems differ substantially and concepts like transparency, accountability and democracy remain contested across time and space. Thus, there is no universal blueprint for intelligence oversight.

Effective intelligence oversight, therefore, remains an ambitious, unattained and vague benchmark - on both sides of the Atlantic. It should be regarded as continuous work in progress and - despite these challenges - much work can be done today to significantly improve oversight effectiveness. This work should not be left to government and legislators alone. As the pace of technological innovation continues to challenge core concepts of intelligence law and oversight practice,[2] a broader set of perspectives are needed to identify and refine options for positive change. It is with this aim in mind that the Stiftung Neue Verantwortung initiated this working group on oversight innovation. Generous support from the William and Flora Hewlett Foundation and the Robert Bosch Foundation allow us to assemble unique expertise. Using collaborative methods, the group aims to identify and refine ideas for

[1] This paper was prepared for the first workshop of the Transatlantic Cyber Forum's track on intelligence oversight innovation.

[2] For example, in 2017, Section 10.4 Art.10 Law still stipulates "Further, the (interception) order shall specify what proportion of the transmission capacity available on these transmission paths may be monitored. In cases pursuant to Section 5 (foreign-domestic strategic surveillance), this proportion may not exceed 20 per cent." It does not specify whether this percentage pertains to the capacity of the cable or the overall percentage of traffic. Much of this has changed as technology moved from satellite to fibre optic cables and concepts such as national and non-national data are increasingly difficult to operationalise.

better intelligence oversight. What changes to the oversight process or the setup of oversight bodies might make a positive contribution to oversight development?

This discussion paper is meant to set the scene for the collaborative work of this group. It discusses a range of current and future challenges to effective oversight over electronic surveillance before flagging areas where potential solutions may be found.

II. Problem Analysis: Contemporary and Future Oversight Challenges

As indicated, many factors can impede effective oversight. Some are very difficult to measure. Some may only be known inside the ring of secrecy. Despite this, one does not need a security clearance to know that many aspects of contemporary intelligence oversight remain unfit for purpose. This section provides examples of practices that do not match the ideal-type of oversight often conveyed in recent national intelligence laws or some oversight reports.[3]

a) Intelligence oversight on the books and on the ground
Overseers need to know the national and international legal framework in which the services operate. They also need to possess sufficient knowledge of modern intelligence practices and the various tools that are being used. Case-law confirms that they need to possess adequate investigatory powers and meaningful access to intercepted or otherwise acquired data by the intelligence community. Their control and sanctioning instruments must allow them to review, access and, where necessary, to rein in the executive and the intelligence community's unnecessary or unlawful practices.

But where do overseers get this kind of knowledge and does their oversight remit and their control instruments provide a sufficient level of relevant information? Who trains them in hard national security questions? In regard to the judicial oversight of electronic surveillance measures: How much information on an interception warrant do these institutions typically have when they authorize a measure? What technological tools do members of the US foreign intelligence surveillance court (FISC), the Dutch independent expert body (CTIVD) or the German quasi-judicial G10 Commission have at their disposal to ascertain that the services' data collection, data minimization, data

[3] Whether or not individual oversight frameworks of different countries are equivalent shall not be discussed here. The "adequacy" of national intelligence oversight systems is an issue that will continue to be relevant in U.S.-E.U. data politics. Yet, this is also highly politicized and not directly relevant to our work that seeks to be beneficial to both sides.

handling and data transfer practices are administered in accordance with the law?

Do members of such judicial oversight bodies have sufficient and timely access to actual - not just reported - intelligence practice when assessing the legality and necessity of individual measures? Is their access and grasp of the technology sufficient to detect potential inconsistencies? Can they obtain additional information and independent expertise to help explain deviations or puzzles (e.g. with regard to the amount and use of incidentally collected data that falls outside the scope of an authorized measure and that minimization procedures are meant to prevent from being acted upon by individual intelligence analysts)? Do overseers have sufficient, independent access to corroborate their findings over time?

Arguably, these are open questions in many countries. The following examples will briefly shine further light on specific instances where oversight practice is not in keeping with the law.

b. Examples of post-reform problems with judicial oversight of electronic surveillance

Even the best regulatory frameworks, of which there are few, can do only so much to guarantee better oversight on the ground. The following examples illustrate this with regard to Germany.

- In 2017, Germany does not meet the standards for independent control of data processing that the Council of Europe's Venice Commission promotes (Venice Commission 2015: para 121).

Exhibit 1- Germany: The remit of the G 10-Commission covers the entire collection, processing and use of the personal data that the Federal Intelligence Service gathers under the Art 10-Law. The G 10-Commission members „are to be given access to any documentation, especially stored data and the data processing software connected to the surveillance measure" (Section 15.5. No. 3 Article 10-Law). What may sound progressive at first, especially given that this law has been in existence for several decades, does, on closer inspection, not result in de facto independent control of intelligence data processing. Aside from the authorization process, the law does not mention any control obligations or control responsibilities. Rather, the four honorary members of the commission are free to also control the manner in which the BND handles the collected data. Provided they wish to do so and have the time for it. This is not the case.

Exhibit 2- Germany: There is no digital trail regarding the decisions of the G 10 Commission on interception warrants and, equally important, the documentation of individual measures by the ministries and the services to implement individual orders. The G 10-Commission is not subject to any public reporting requirement as regards its work.[4]

Exhibit 3 - Germany: The four members of the G 10-Commission meet only once a month. Realistically, this leaves little time to properly decide on the admissibility and necessity of interception warrants, let alone to conduct examinations in the field of data protection.

Exhibit 4 - Germany: All foreign-foreign strategic surveillance measures recently codified in the 2016 amendment to the BND-Law require a collection order. Yet, depending on the different groups that these measures can be aimed at, the collection order may not mention the specific search terms that are being used by the BND to obtain specific information from the entirety of data acquired by its strategic surveillance. A judicial review of the actual practice is much less meaningful without actual knowledge of the search terms used.

Exhibit 5 - Germany: The German constitution guarantees the right to private communication as a fundamental right (not only to German citizens). Whether or not this right is protected in practice depends to a large degree on the accuracy of the data minimization / filter process. During the NSA-Inquiry Committee the three-tier DAFIS filter program was discussed in public. Irrespective of the important question whether the filters are producing accurate results or not, the very filter management and reporting requires overseers to trust the information they receive. There is no independent verification or control of the filter programs.

These are just a few of many possible examples. Similar examples of oversight deficits can be found in other countries.[5] Another oversight deficit that all countries share is the limited national oversight that exists in regard to international intelligence cooperation. Whereas security and intelligence agencies face fewer and fewer legal and practical obstacles to engage in ever more profound forms of cooperation, national institutions of democratic control and oversight fail spectacularly to follow suit. To date, there are no effective institutions, networks, platforms or databases for international oversight cooperation. Instead, national overseers adhere to strict national confines when they perform their critical review and control activities.

In the UK, it seems worth asking whether the four bulk powers of the Investigatory Powers Act need further "trimming".[6] In the US, recent debate revolved around so-called "backdoor search loopholes". Also, it is noteworthy that the collection under Executive Order 12333 occurs "entirely outside of the

[4] The relevant ministries, not the G 10-Commission, inform the Parliamentary Intelligence Oversight Body (PKGr) about interception orders. The PKGr then informs the Bundestag on a yearly basis on the "execution as well as type and scope" of the surveillance measures.

[5] If you would like to submit "exhibits" pertaining to the challenges to administer effective intelligence oversight on electronic surveillance measures, please send them to us.

[6] See for example, the interesting discussion here: http://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html

province of FISC review. And the administrative rules that govern the uses of information involving domestic or U.S. persons acquired under Executive Order 12333 do not receive any judicial review" (Daphne Renan).

Future challenges to effective oversight

Below, the text briefly accounts for a number of future oversight challenges. Surveillance laws have become more complex. We will not have the time nor the resources to discuss individual amendments or new laws exhaustively here. Arguably, though, a number of themes stand out.

#1 Minimization & Safeguards for data processing

Oversight and safeguards for data processing has not received the kind of attention it deserved. Recent legislative efforts rightly focused on the mandate of the intelligence and security services to engage in different bulk powers and the authorization process that comes with it. Yet, as the recent scandal with regard to the accreditation refusal of some journalists at the G-20 proceedings in Hamburg show,[7] there needs to be a better framework and operational process in place for the independent scrutiny of data use by the intelligence and security services. Did the services only collect that what was stated in the warrants? Did they tag the collected data in accordance with the purpose that the interception order initially foresaw?

"Especially for the processing of increasing amount of data, additional and future-proof safeguards are necessary. These safeguards must pertain to the phase of the data processing in which privacy (and other rights) is/are actually infringed, i.e. during the automated processing, analysis and use phase." CTIVD Annual Report 2016

As indicated, in some countries overseers still do not seem to get involved much with data processing safeguards. Once judicial oversight bodies have signed off a particular interception order there may not be a digital trail that one can subject to independent data processing audits. That is to say, once a warrant has been cleared, the ministries and security agencies may only produce paper trails regarding the implementation of a particular order.

#2 Effectiveness evaluation

There have been a few attempts to evaluate the effectiveness of some surveillance policies in some countries but, generally speaking, there is a lack of publicly available evidence to attempt different models and little agree-

[7] Journalists were denied access due to data processing errors. Data that should have been deleted or amended in the files remained unchanged in key databases. While this case concerned the Federal Police Agency (Bundeskriminalamt - BKA) and not the German intelligence services, it points to the risk of having insufficient scrutiny over data processing. This point can be made with regard to the German intelligence agencies but also with regard to the growing "Security Union" that is being build in and around Brussels.

ment about how to measure and quantify effectiveness. Given the costs and the invasiveness of modern surveillance tools, and given that the legitimacy of national intelligence services depends on both in-put (i.e. accountability mechanisms) and out-put (i.e. effectiveness of operations and tools), it is necessary to try harder and to create a better knowledge base. In fact, some European oversight bodies (such as the Belgian independent oversight committee) are mandated to review the effectiveness of their intelligence services, but they lack objective indicators to conduct verifiable assessments. In the US, both PCLOB and the "Committee on Responding to Section 5(d) of Presidential Policy Directive 28" have done essential work here.[8]

#3 Cyber Security and Counterterrorism - Different data needs, same oversight?

When it comes to securing critical infrastructures against various cyber threats, many surveillance laws allow their security and intelligence agencies widespread search mandates. At the same time, recent surveillance laws introduced a more specific set of requirements for the collection of counterterrorism data by means of electronic surveillance. Therein lies a challenge for agencies, and by extension for oversight bodies, namely to engage in data minimization and filtering whilst at the same time allowing wide searches against potential cyber threats. Examples for simultaneously broad and narrow mandates can be found in recent amendments to the Dutch and the German surveillance laws.[9]

#4 Filter governance, incidental collection and queries upon queries

This year, the NSA decided to halt its "about collection" under Section 702, partly because "a problem with analysts queering the fruits of that collection in a manner that departed from what the FISC had approved" (Robert Chesney, Lawfare Post, April 28, 2017). Irrespective of the "about collection" issue, there are also questions with respect to the queering authority. Much data is shared with different intelligence and law enforcement agencies. The very practice of queering databases can be problematic if insufficiently processed data becomes readily available to agencies with kinetic powers.

Aside from the need for an independent review of filters to prevent large-scale privacy violations, it may also be in the interest of judicial review bodies to invest more attention to this. Many countries have an individual notification obligation if rights-holders were subjected to electronic surveillance. This

[8] See their report Bulk Collection of Signals Intelligence: Technical Options (2015).

[9] For example, in Germany, Section 5.1 Nr. 8 of the Art-10-Law includes a very broad mandate to use strategic foreign-domestic surveillance against potential cyber threats whereas Section 6 and Section 9 of the BND Law purport to limit the possibility of Germany's foreign intelligence service to collect data. See also Lawfare post New Rules for SIGINT Collection in Germany

task could become overwhelming if incidental collection exceeds in size and nature.

#5 Intelligence activities outside the "intelligence community" and the risk of collusive delegation

Enormous investments in technology and the gradual convergence of surveillance hard- and software mean that military, intelligence and police missions become increasingly intertwined both nationally and internationally. Against the backdrop of interconnected national security and intelligence activities, it is a problem when oversight law and practice focus solely on a fraction of the entirety of intelligence activities conducted by or on behalf of the government. For example, the German oversight laws mandates parliamentary and quasi-judicial review only with respect to the three federal intelligence agencies. However, intelligence activities by the German Armed Forces, the Federal Police and the newly established cyber security institutions (such as ZITiS) are not subject to the same kind of oversight (if any). This may invite creative non-compliance or collusive delegation. An example would be that competencies are being transferred from BND to the Armed Forces or even to new multilateral European institutions in the future. There can, of course, be many reasons for such delegations. One explanatory factor might be that oversight is less rigid at the institution to which competences are being delegated to. At any rate, new thinking on how to ensure a competent review of intelligence activities across government is needed. Arguably, Canada has moved furthest in this regard.[10]

#6 Metadata/secondary data/hacking and oversight

The recent German law on foreign-foreign intelligence collection received some international attention for its provisions limiting the collection of data from non-nationals, enforced in part by a new judicial oversight mechanism. Irrespective of this, there are a number of things that the law does not address. Unlike an earlier draft of the bill, the law does not set limits regarding the collection, use and transfer of metadata. Similarly, Graham Smith finds that "the IPAct is almost completely devoid of concrete limitations on, or distinctions between, the types of use that can be made of bulk metadata. The limits are the statutory purposes, operational purposes and necessity and proportionality."

These are just a number of future challenges regarding effective oversight for electronic surveillance. If you want to discuss other additional challenges or would like to comment on the above, please do.

[10] See in particular the discussion on policyoptions.irpp.org .

III. Ideas for oversight development

What can those outside the ring of secrecy do to make the threat of defunct intelligence oversight loom less large? Unsurprisingly, many people would advocate that technology should be put more readily at the disposal of oversight bodies. As intelligence and security services are pioneering digital tools for their work, what tools may put overseers in a better starting position?

The following section flags ideas that we deem relevant for our work on oversight innovation. We look forward to other suggestions you may have. The suggestions are currently grouped into two separate categories but our ideas and categories will be subjected to critical review. Please send us specific comments and we will integrate them into our plan for the next meeting of our working group.

Technology is the answer. (What was the question?)

Ideas for oversight development that touch upon a more systematic use of technology (writ large) are grouped into the first category. Some of the following ideas originate from earlier discussions with individual participants of the Transatlantic Cyber Forum. In particular, I would like to give credit to Eric King, Jörg Pohle, Klaus Landefeld, and Graham Smith.

#1: Continuous digital documentation of all activities linked to authorized interception orders

Overseers should have more readily available access to the entirety of surveillance measures that are currently running when they are being asked to authorize new surveillance measures. One idea would be to create a digital trail for all current surveillance measures. Those responsible for acting upon an authorized interception order will have to put all activities in numerical order and must include all the necessary metadata information concerning each individual activity (duration, initial purpose, data collected, etc.) Such data should then be made available to oversight bodies and they must be obliged to conduct random samples on this database. Has a particular surveillance measure provided sufficient information since it was first initiated? How many other measures are currently pursuing similar goals or are also infringing on the privacy rights of individual targets? These questions are not often part of the authorization and data processing reviews. A better digital trail would help here. This can also be tied to the “Überwachungs-Gesamtrechnung" (total count of surveillance measures) concept developed by the German Constitutional Court.[11]

#2 Quantifying intrusion of modern bulk SIGINT techniques

The majority of laws regulating the use of SIGINT techniques are predicated on a two stage authorisation framework where initial warranty is sought for large scale accesses, with a second authorisation process when an intelligence officer wishes to view the collected information (usually only required if viewing material of a citizen). This authorisation model often fails to take into account interference with rights in between these two stages caused by the use of modern 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-focussed datasets. As these techniques become more widespread, a common understandings of how and where privacy intrusion occurs and is impacted will be essential to ensure 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 measurement to just how significantly an individual privacy is interfered with. What models and tools could we borrow from the business sector to quantify privacy intrusion?

#3 Additional criteria for authorizing surveillance measures

The traditional norms of proportionality and necessity can be difficult to translate to our digital times and big data. Sometimes we may also need to rethink some assumptions. Should, and if so how, can statistical accumulations / thresholds play a more prominent role in surveillance policy and the authorization and oversight of individual measures?

#4 Oversight Interfaces

This idea would adapt Lawful Interception Interfaces (LII) for oversight purposes: Whereas LII is installed in communication backend systems to allow access for LEA and SIS, one could envision similar interfaces being added to the LII tool. Whereas LII are not controllable by the carriers, the interfaces added to LII might not be controllable only by overseers and not by LEA and SIS. Yet, how to standardize/certificate such oversight interfaces? By whom and for what data? How to persuade all stakeholders (standardizing authority; producer; carrier/ISP providers; LEA and SIS; oversight bodies; parliaments, etc.) involved to build and apply such tools? Alternatively, is it enough to get the producer to build such an oversight interface by default and over

[11] see: Roßnagel, Alexander: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, Neue Juristische Wochenschrift 2010, 1238

time this may increase pressure for politicians and security professionals to accept change?

#5 Audit Studies for SIGINT Oversight Bodies

What viable options are there to improve the quality and quantity of access to data collection and data processing? How can overseers monitor that the software used to collect, filter and analyze SIGINT is implemented and applied in a lawful and effective way? Well, oversight bodies could conduct audit studies. Auditing is a way to determine what a black box software system is doing. The agencies would not have to make their methods transparent, yet they would have to give direct software access to oversight, for example as a API with specific data access that can only be used for this kind of audit. It is a way to check systematic biases by addressing polarized examples to real decision-making systems (e.g. to test data about German citizens abroad that should be filtered out and/or masked or to test the presumptions of threats). The audit is an ex-post oversight measure that must be operated without informing the services about the "when, how, and why" before. Tests that oversight bodies could run could include: Are filter systems as accurate as the government/agencies claim? Or is the rate of false positive much higher than indicated? How does the system behave if confronted with random data sets? Do biases occur in the output that should not appear in a random data set? As regards the latter two questions, one may conduct a "sock puppet audit". This would mean that oversight bodies use "fake" data to test how the system behaves and whether it does what it is designed to do. Intelligence agencies might consent to such an audit as a trust-building measure.

At present, oversight bodies in many countries rely too often directly on the data that the agencies provide. An audit could do randomized tests of the system, like financial auditors perform random controls with your accounting data. This could increase compliance and provide incentives to build more accurate and diligent software tools.

An audit would only make sense, of course, if the results can be compared to efficiency standards. This would require a broader societal discussion about what the acceptable (legal and effective) behavior of the SIGINT software system ought to be in practice. This audit would also require oversight access to the collection tools and filter programs used by the security agency (i.e. Xkeyscore, DAFIS). Ideally, audit results should then also be included to the extent that is possible in public reports on the oversight work.

#6 Homomorphic Cryptography

It is possible to do ALL the data processing on encrypted data, producing an encrypted result without exposing the data in the clear. Oversight staffers would also hold one key to such encrypted data. See the video clip shown at the workshop.

Regulatory interventions or other non-technical ideas for oversight development

#1 Stronger Safeguards in Intelligence Laws

The idea here would be to strengthen the safeguards that exist in the data processing process where much of the privacy infringement actually take place, i.e. during the automated processing, analysis and use phase. This could cumulate in recommendations for amended intelligence laws, including extra warrant procedures for "strong selectors" (Graham Smith)
"Isolate collected data" and "restrict queries" (as discussed in the report "Bulk Collection of Signals Intelligence: Technical Options (2015).

#2 Duty of Care Provision in Intelligence Laws

In the Dutch intelligence bill, a new provision was introduced. It obliges "services to give account of the quality of the automated processes for data processing by means of instruments laid down by law; and that this quality can be reviewed effectively. " (Rough Translation from the Dutch bill)

#3 Responsible Data Reduction

The data should be collected in the most targeted manner possible and the data collected must be reduced as soon as possible to the data actually required by intelligence and security services. Embedding purposiveness of data processing to ensure that interception and further processing are actually related to individual investigation assignments, that the storage of data is limited as a result and that destruction of data takes place in a timely fashion and also that this can be reviewed effectively.

- "seeded analysis vs more generalised pattern detection" (see discussion by Graham Smith)[12]

The ideas presented above served as a springboard for the first workshop of the Transatlantic Cyber Forum on oversight innovation.
We look forward to your feedback and welcome any additional thoughts you may have.

[12] http://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html

About Stiftung Neue Verantwortung

The 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.

The Transatlantic Cyber Forum (TCF) has been established by the Berlin-based think tank Stiftung Neue Verantwortung (SNV). The TCF was made possible by the financial support of the Robert Bosch Stiftung and the William and Flora Hewlett Foundation.

About the Author

Thorsten Wetzling directs the Privacy Project. His current research and advocacy focuses on the democratization and professionalization of intelligence governance in Germany and Europe. Thorsten testified before the European Parliament and the Bundestag on intelligence legislation and his recent work appeared in various German media outlets, including the Frankfurter Allgemeine Zeitung, Der Spiegel, Zeit Online, Frankfurter Rundschau and Handelsblatt. Thorsten holds a doctorate degree in political science from the Graduate Institute of International and Development Studies in Geneva. Previously, Thorsten worked as Senior Fellow at the Brandenburg Institute for Society and Security, The Hague Institute for Global Justice and as Advisor for the Geneva Centre for the Democratic Control of Armed Forces (DCAF). As Transatlantic Post-Doc Fellow for International Relations and Security (TAPIR), Thorsten also conducted surveillance policy research at the French Institute for International Relations (ifri) in Paris and the RAND Corporation and the Center for Transatlantic Relations at Johns Hopkins University in Washington, D.C.

Contact:
twetzling@stiftung-nv.de, Twitter: @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

Kostenloser Download:

www.stiftung-nv.de