December 2021 · Thorsten Wetzling, Lauren Sarkesian & Charlotte Dietrich

Solving the Transatlantic Data Dilemma

Surveillance Reforms to Break the International Gridlock

Stiftung Neue Verantwortung

OPEN TECHNOLOGY INSTITUTE

Think Tank at the Intersection of Technology and Society

Abstract

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the European Commission's adequacy decision for the EU-U.S. Privacy Shield framework in the Schrems II case—which until then, regulated transatlantic exchanges of personal data for commercial purposes—because U.S. surveillance law provides inadequate safeguards for EU citizens' data. Since then, many companies have been left questioning the future of transatlantic data flows while the United States and EU Commission negotiate a successor agreement. The two have not yet announced a path forward.

Establishing a new agreement for transatlantic data flows is incredibly complex. What common norms and standards should be written into a new agreement to assuage valid concerns on both sides about disproportionate government access to personal data? This report points to the heart of the current transatlantic data transfer dilemma: the governance of foreign intelligence collection and the many unresolved questions regarding the protection of fundamental rights in cross-border contexts. Reviewing recent jurisprudence and surveillance reforms in several democracies, much more needs to be done—both in the United States and across Europe—to better protect the rights of non-nationals from disproportionate government access. Our report focuses first on direct and compelled access through bulk collection by intelligence agencies before examining voluntary access to data held by the private sector, and finally, other inter-agency data transfers.

This report includes recommendations or steps that governments can take to better meet evolving international standards of necessity and proportionality. While it is neither possible nor desirable for democracies across the globe to adopt the same standards for proportionate government access to data irrespective of their different constitutional systems and heritage, more robust safeguards are necessary to ensure the free flow of data with trust to resume.

Acknowledgements

Several people offered their time, advice, and expert knowledge to us. We owe tremendous gratitude also to Lisa Johnson, Austin Adams, and Corbinian Ruckerbauer for their excellent editorial assistance. We are also grateful to Professor Théodore Christakis, Chair AI-Regulation.com, Université Grenoble Alpes, Member of the French National Committee on Data and AI Ethics, for his constructive feedback on an earlier draft of this text. Finally, we want to thank the experts that participated in the three thematic workshops on cross-border data transfers and intelligence legislation for their active participation earlier this year. We are solely responsible for the contents of this report and the views and opinions expressed therein do not necessarily reflect those of the workshop participants and reviewers. This research was in part funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation - Project Number 396819157)

Executive Summary

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the European Commission's adequacy decision for the EU-U.S. Privacy Shield framework, which until then, regulated transatlantic exchanges of personal data for commercial purposes. In Data Protection Commission v. Facebook Ireland (Schrems II), the CJEU argued that U.S. surveillance law provides inadequate safeguards for EU citizens' data. This was a transatlantic bombshell, as it left thousands of companies questioning the future of their transatlantic data flows. Since then, the United States and EU Commission have been negotiating a successor agreement, but have not yet announced a path forward.

Establishing a new agreement for transatlantic data flows is incredibly complex. Legal frameworks for different modes of government access to personal data as well as obligations for data processing, transfers, retention, deletion, and redress mechanisms vary substantially—even within Europe. What common norms and standards should be written into a new agreement to assuage valid concerns on both sides about disproportionate government access to personal data?

This report points to the heart of the current transatlantic data transfer dilemma: the governance of foreign intelligence collection and the many unresolved questions regarding the protection of fundamental rights in cross-border contexts. Reviewing recent jurisprudence and surveillance reforms in several democracies, the report shows that much more needs to be done—both in the United States and across Europe—to better protect the rights of non-nationals from disproportionate government access. Our report focuses first on direct and compelled access through bulk collection by intelligence agencies before examining voluntary access to data held by the private sector. While intelligence legislation and practice is the main focus of this report, we also review law enforcement or military agencies' access to data, albeit mostly in conjunction with governance and policy questions tied to inter-agency data transfers.

Each chapter of this report includes recommendations or steps that governments can take to better meet evolving international standards of necessity and proportionality. While it is neither possible nor desirable for democracies across the globe to adopt the same standards for proportionate government access to data irrespective of their different constitutional systems and heritage, more robust safeguards are necessary to ensure

the free flow of data with trust to resume. This will stimulate growth among our digital economies and strengthen our democracies. Some recommendations are long-term goals that require bold legislative action; others can be achieved in the medium term without substantial reform of legal frameworks. We do not argue that all the measures we recommend are strictly required by the *Schrems II* decision, or that any particular reforms would resolve the CJEU's concerns. Rather, we identified a broad package of reforms that could help to prevent a future halt of transnational data flows.

Table of Contents

Chapter 1

Introduction

Much of modern life relies upon a wide range of digital services and platforms. From smartphone apps to email services and beyond—these tools and programs all collect our data, some of which is quite sensitive. In our interconnected world, that data may very likely also be transferred to other jurisdictions for further data processing or storage. While most of us may not even realize this transaction happens, it can interfere with our basic rights in several ways.

Domestically, national security agencies may access personal data as part of their mandate to protect national security. While this tends to be a densely regulated space in democratic states, lawmakers, national security professionals, courts, and civil society often find it challenging to ensure that legislation and practice provide both individual rights protection and national security. This is a matter of frequent policy debates, political battles, and reform.

Cross-border data transfers raise the same issues and can cause the same interferences with basic rights, albeit by the private and state authorities of another country. In theory, this necessitates a similarly appropriate balance of strong standards to protect personal data against unconstrained and disproportionate government access. Until recently, though, safeguarding rights in the context of cross-border data transfers was not satisfactorily addressed.

In July 2020, the European Court of Justice invalidated the European Commission's decision regarding the EU-U.S. Privacy Shield, and thus brought new attention to this issue. In its landmark Schrems II judgment, the court assessed the adequacy of U.S. intelligence law and practices, questioning whether they provide an essentially equivalent standard to European data protection and privacy law. The court held that "neither Section 702 of the FISA, nor EO 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of Proportionality" and concluded that U.S. "surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary."[1]

1 Court of Justice of the European Union. Schrems II Judgement. July 26, 2020, recital 184. https://data.guardint.org/en/entity/k4ae1290jz?searchTerm=effective&page=39

While this caused the European Commission and the U.S. government to privately address cross-border data flows, data protection, and government access to data with greater urgency again, there is a much greater need to publicly explore and debate a wide range of policy questions. For example, what type of data processing, by whom, may be allowed for what kind of non-national data? For which aims, and according to which safeguards? Who should set those standards, and who should oversee them? Can they be challenged, and if so, how?

Amid the current transatlantic data gridlock, enormous economic and political interests that are tied to the free flow of data hang in the balance. For example, the increased difficulty in transferring data could result in data localization. This practice, which has been on the rise in recent years, has detrimental economic and societal impacts across the globe, fragmenting the internet as we know it and interrupting global communications and a wide variety of other services.

The United States and the EU have the opportunity to set an example for how cross-border data transfers can exist without compromising human rights. It is important that they get this right, as they risk losing ground to authoritarian regimes that are far less concerned with high standards and safeguards for data processing.

Being leaders in cross-border data transfers will require a more sustainable effort to address and mitigate the wide range of concerns, risks, and dangers that are associated with insufficiently regulated and inadequately overseen cross-border data transfers and respective government access. A prior iteration of the EU-U.S. Privacy Shield also failed to meet sufficient standards and was invalidated by the European Court of Justice in 2016.[2] A more durable agreement is needed to satisfy not just policymakers, but individuals and judiciaries for the long term. In this report, we will focus, in particular, on concrete risks to digital rights that transatlantic policymakers should address to resume the "free flow of data *with trust.*"[3]

Chapter Two of this report lays out that the law has a lot of catching up to do with the rapid evolution of digital surveillance. On both sides of the Atlantic,

2 Court of Justice of the European Union. Schrems I Judgement. October 6, 2015. https://data.guardint.org/en/entity/x4n55jjny1k

3 OECD Committee on Digital Economy Policy. "Government access to personal data held by the private sector." 2020. https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

opaque legal frameworks for surveillance and intelligence make it difficult for individuals to understand and enforce their rights.

Chapter Three highlights how governments' access to commercially available data remains a frontier of law and policy on both sides of the Atlantic.

Chapter Four discusses how additional risks to lawful and legitimate cross-border data transfers stem from the fact that much of the hardware and software used by the security sector converge around similar products and facilitates automated data sharing and cross-system information analysis.

The report's main focus lies on intelligence agencies' access to personal data.[4] Each chapter raises serious accountability risks and critical policy questions about government responsibilities that ought to be addressed more rigorously by transatlantic policy circles.

The Current State of EU-U.S. Surveillance Negotiations

Policymakers on both sides of the Atlantic have been cooperating with renewed vigor as part of the EU-U.S. Trade and Technology Council (TTC) that met for the first time in Pittsburgh in September 2021. The council formed 10 working groups to "carry forward important work to strengthen our relationship and cooperation." They focus, among other things, on topics like "data governance and technology platforms" and "misuse of technology threatening security and human rights" (e.g., "arbitrary and unlawful surveillance"). [5]

EU officials attending the inaugural TTC meeting in Pittsburgh confirmed that "data flows" were not on the official agenda.[6] By early December 2021, after months of bilateral negotiations on a future EU-U.S. data agreement, no precise path forward, let alone successor agreement, has been announced. However, the fact that European Commissioner Didier Reynders might not meet his objective "that a successor agreement to Privacy Shield could be

4 We are aware that law enforcement agencies' access to personal data is an equally pressing theme in transatlantic policy circles, particularly with regard to trans-border access in the context of criminal investigations. Examining this further would have gone far beyond the scope of this report.

5 EU-US Trade and Technology Council. "Joint Statement". September 29, 2021. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951

6 Manancourt, Vincent and Mark Scott. "Washington says a transatlantic data deal is close, Brussels disagrees". *Politico*. September 17, 2021. https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/washington-transatlantic-data-deal-brussels/amp/

reached by the end of 2021," may be good news because it will allow policymakers to engage in inclusive policy debates on the many complex and pressing questions regarding proportionate government access to personal data.

Safeguarding data amid transatlantic data transfers is incredibly complex, and negotiators are right to aim for an agreement that is legally defensible.[7] Additionally, U.S. and EU citizens need greater clarity into evolving surveillance practices, the laws that govern them, and the oversight bodies involved. We suspect that the many open policy questions and democratic deficits identified in the following three chapters are, at least in part, the result of a long-standing preference—both in the United States and across Europe—to shy away from addressing the complicated nuances and open questions of government surveillance. Unless these matters are addressed in more inclusive policy debates that result in more comprehensive legislative reforms, we are concerned that the United States and EU might not be able to resume the transatlantic free flow of data *with trust*.

7 Palmer, Doug. "U.S. Wants 'Legally Defensible' Privacy Shield Pact, Commerce Negotiator Says." *Politico Pro*. July 20, 2021.

Chapter 2

Foreign Intelligence Collection and Data Transfers

The link between a company's handling of customer data and government surveillance became far more prominent after Edward Snowden's revelations in 2013 and subsequent inquiries into similar practices by EU member states. In July 2020, the European Court of Justice (CJEU) invalidated the Privacy Shield in the *Schrems II* case, finding that several U.S. surveillance authorities—specifically, Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 12333)—do not provide an adequate level of protection for EU citizens' data,[8] and that the United States lacks a mechanism for meaningful redress for EU citizens whose data is transferred to the United States. This was a big moment for transatlantic policymakers and the private sector alike: over 5,300 companies relied on the Privacy Shield for data transfers between the United States and Europe for services including social media, messaging, cloud services, email, and beyond.

After the court struck down the Privacy Shield, the European Commission began engaging in another attempt at a binding agreement on cross-border data flows and data protection standards regarding government access with

8 The CJEU referred to several U.S. intelligence collection programmes:
"60. [...] the US authorities' intelligence activities concerning the personal data transferred to the United States are based, inter alia, on Section 702 of the FISA and on E.O. 12333.
61. In its judgment, the referring court specifies that Section 702 of the FISA permits the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not United States citizens located outside the United States in order to obtain 'foreign intelligence information', and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes. In the context of the PRISM programme, Internet service providers are required, according to the findings of that court, to supply the NSA with all communications to and from a 'selector', some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA).
62. As regards the UPSTREAM programme, that court found that, in the context of that programme, telecommunications undertakings operating the 'backbone' of the Internet — that is to say, the network of cables, switches and routers — are required to allow the NSA to copy and filter Internet traffic flow in order to acquire communications from, to or about a non-US national associated with a 'selector'. Under that programme, the NSA has, according to the findings of that court, access both to the metadata and to the content of the communications concerned.
63. The referring court found that E.O. 12333 allows the NSA to access data 'in transit' to the United States, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. It adds that activities conducted pursuant to E.O. 12333 are not governed by statute." Schrems II

the U.S. government.[9] With its decision, the court provided a clear emphasis on genuine safeguards against disproportionate government access and judicial redress for European data.

Coming to a new agreement is by no means an easy task, for a wide range of reasons. Given that the CJEU refrained from any direct comparisons of U.S. intelligence legislation with EU member state intelligence laws in its *Schrems II* decision, there is an understandable demand that a future agreement be evenly analytical. Thus, U.S. customers of digital services should receive the same protection against disproportionate government access and the chance of effective remedies for the processing of their data in Europe. However, ensuring this reciprocity is beyond the competence of the European Union and can only be decided by individual EU member state in their national laws on surveillance.

Policymakers need to flesh out how the abstract data protection standards used in the CJEU's *Schrems II* ruling can be applied in concrete situations of intelligence collection and data processing as well as how they should be written into national intelligence legislation. We need more clarity and concrete examples of good practice as it relates to questions of adequate safeguards, disproportionate government access to communications data in foreign intelligence collection, and more. It is often easier to determine where a legal provision is underwhelming than to concoct better standards, both across Europe and in the United States.

There are three common points of friction that originate from the legal frameworks and oversight practices on foreign intelligence collection in several EU Member States and the United States. First, there is a lack of safeguards in intelligence legislation regarding the re-use of personal data (purpose limitation) and the transfer of collected data to foreign services (unconstrained intelligence cooperation). Second, there is insufficient protection of non-nationals in intelligence legislation. Third, there is ineffective review and oversight practice on foreign intelligence collection and data transfers. This section will introduce each of these issues and their relevance for transatlantic cross-border data transfer consultations. It also explores potential solutions to these points of friction.

9 For more information on the trajectory of the European Court of Justice's previous decisions on EU-US data transfer agreements, see for example: Tzanou, Maria. "Schrems I and Schrems II: Assessing the Case for Extraterritoriality of EU Fundamental Rights." October 13, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3710539

A. Insufficient Purpose Limitation and Data Transfer Safeguards in National Intelligence Legislation

1. Problem Analysis

There are not enough safeguards written into national surveillance legislation in many countries to prevent the repurposing of data obtained from foreign intelligence agencies. Imagine a situation where data is lawfully being collected in bulk by a European intelligence agency for the purpose of informing its government about political developments in the Western Balkans (purpose A). And imagine then that that data is then being used, without additional authorization, for counter-terrorism finance tracking purposes (purpose B). Consider, also, that the data collected in bulk for purpose A is then used by the European intelligence service to request intelligence from the Swift Network for purpose B. Initiation of such a request means passing the data onto the U.S. Treasury Department to run searches on the basis of these requests.[10] In doing so, the data collected by the European intelligence agency may end up in U.S. databases where other U.S. services may be able to access and use the data for different purposes. Alternatively, the data initially collected in bulk by one European intelligence agency for purpose A could also be shared in an unevaluated and automated fashion with additional foreign intelligence agencies who may process such data for other purposes.

The re-use of data within the government for a different purpose and the sharing of such data with foreign intelligence partners would, according to European courts, constitute a separate interference with fundamental rights and consequently require independent statutory protections that are necessary and proportionate.[11] Therefore, national intelligence law should include specific safeguards to make these additional uses lawful and legitimate.

10 Tau, Byron. "EU Leans Heavily on U.S. Program Tracking Terror Financing." *The Wallstreet Journal.* November 19, 2020. https://www.wsj.com/articles/eu-leans-heavily-on-u-s-program-tracking-terror-financing-11605794404 and Klein, Adam. "Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program." *PCLOB*. November 19, 2020. https://documents.pclob.gov/prod/Documents/Projects/96bd2a55-ea48-4426-8b5f-06571ce7c357/TFTP%20Chairman%20Statement%2011_19_20.pdf

11 According to the CJEU in the Schrems II decision, "the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the [European] Charter [of Fundamental Rights], whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference." In: Court of Justice of the European Union. Schrems II Judgement. July 26, 2020, recital 171. https://data.guardint.org/en/entity/k4ae1290jz?page=38

However, this is an abstract requirement that needs to be broken down into specific intelligence governance contexts. For instance, questions to consider include, "does this require separate authorization procedures and binding obligations on the government to seek assurances from the foreign government that the data will only be used for purposes that are lawful,?" and "how would one obtain binding assurances in a context that pertains to the heart of national sovereignty?"

Recent jurisprudence on legal frameworks for intelligence collection in Europe (notably in the U.K., Sweden, and Germany) and subsequent legislative reforms (Germany) give indications as to how to establish and maintain new and potentially more effective safeguards, and should be considered within the context of current U.S.-EU consultations on cross-border data flows and data protection standards.

For example, the May 2021 decision of the European Court of Human Rights in the *Centrum för Rättvisa vs. Sweden* case, which examined the legal mandate for bulk collection by Sweden's National Defense Radio Establishment (FRA), provides a useful case study. The court acknowledged the possibility that the FRA would share its intelligence with foreign partners sometimes under unpredictable circumstances,[12] and that therefore the precise scope of intelligence sharing cannot fully be circumscribed within the law.[13] However, the court held that the existing law failed to require the FRA to assess the necessity and proportionality of its intelligence sharing with a view to its compatibility with fundamental rights.[14]

2. Roadmap toward Positive Change

In Sweden and beyond, national intelligence legislation should be subjected to further scrutiny regarding its suitability to provide sufficient protection when it comes to data re-use and data transfers. In response to this need, the below discusses six examples of how different policymakers and courts have tried to mitigate the risks of disproportionate government use of personal data.

12 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 322. https://data.guardint.org/en/entity/wdwrxl9tv6f

13 Ibid., recital 323

14 Ibid., recital 322-326

a. Separate Data Collection Regimes in Foreign Intelligence Legislation

One example of having separate data collection regimes in foreign intelligence legislation comes from Germany. Recognizing the many risks of non-compliance and rights infringements—intentional or not—the German Constitutional Court found fault in the 2016 Law on Germany's Foreign Intelligence Service (BND Act) provisions on data transfers and intelligence cooperation. It requested that the German Bundestag amend the BND Act by the end of 2021. In so doing, it formulated minimal conditions that a future legal framework should meet. For example, it requested to limit the conditions in which sharing personal data that stems from strategic surveillance is permissible, and provided specific exemptions. [15]

More specifically, it called for separate data protection regimes in Germany's foreign intelligence legislation depending on whether the purpose of the data collection was to provide political intelligence to the federal government or provide early threat detection. Regarding the former, the court placed restrictions around sharing with domestic or foreign agencies for other—especially operational—purposes,[16] noting that in those cases the intelligence cannot be shared with other bodies. The exception to this is in cases of immediate danger to a person, vital public interests, or security.[17]

The amended BND Act now requires a prior written application wherein the government must state which lawful aim it pursues with the requested strategic foreign intelligence collection. According to §19 BND Act, this can be one of the following two general cases: gathering information for the federal government of Germany (aim one) or detecting threats of international relevance (aim two). Applications for aim one can be authorized if they serve the purpose of obtaining information about foreign countries, are relevant for German foreign and security policy, and are ordered by the Federal Chancellery. By contrast, applications for aim two can be authorized if they satisfy the criteria required for aim one *and* if they can indicate that the foreign intelligence collection

15 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, Headnote 6. https://data.guardint.org/en/entity/neb3eo8hl9h

16 Ibid., recital 226.

17 Ibid., recital 217.

might produce insights into eight general threat areas, or yield insights that allow protection of five legal interests.[18]

The benefit of this practice of distinguishing between the different purposes of data collection is that it adds a powerful deterrence to intelligence services not to share some types of data with foreign services unless it meets specific qualifications related to severity and danger. This practice also requires the positive step of requiring documentation to independent oversight bodies.

b. Stronger Safeguards for Protected Professional Communications and the Core of Private Life

The amended BND Act of March 2021 now also includes stronger safeguards for data originating from either protected professional communications and what the German constitutional court refers to as the *core of private life (Kernbereich privater Lebensgestaltung)*. It also contains provisions to better protect the right to privacy of correspondence, posts and telecommunications (Art. 10 of the Basic Law), press freedom (Art. 5 of the Basic Law), and the right to informational self-determination, as well as the confidentiality and integrity of IT systems in specific foreign intelligence collection contexts. [19]

With respect to protected professional communications, such as for lawyers and journalists, the court created thresholds that must be met in future German foreign intelligence legislation to ensure that surveillance of such communication is limited to investigations of serious threats to individuals,

18 The requirement in § 19 (4) BND Act (our translation) is that "factual indications that these strategic surveillance measures can either produce insights into the following eight threat areas (national defense as well as protection of (allied) armed forces abroad; crises abroad and their effects; terrorism and (violent) extremism, or its support; criminal, terrorist or state-sponsored attacks on information technology systems by means of malware, or support for such attacks; organized crime; international proliferation of weapons of war; as well as unauthorized foreign trade with goods and technical support services in cases of significant importance; threats to critical infrastructures; hybrid threats) or if they produce insights that help to protect the following five legal interests (life or freedom of a person; existence or security of the Federal Government or a state (Land); existence or security of institutions of the European Union, the European Free Trade Association or NATO or a member state of these organisations; the Federal Republic of Germany's ability to act in foreign policy; important legal interests of the general public).

19 For a more comprehensive review, see: Kilian Vieth-Ditlmann and Thorsten Wetzling. "Caught in the Act? An analysis of Germany's new SIGINT reform." 2021. https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform.pdf

criminal activity, or to apprehend dangerous criminals.[20] However, the court offered a compromise to the German government. If the collection of communication data from protected professions takes place with a view to provide political intelligence to the government, less stringent data protection safeguards can apply. In turn, however, this requires that the sharing of such data with other (foreign) partners must be ruled out in principle.[21]

German foreign intelligence law now offers stronger protections regarding the *core of private life*. In practice this means that communications of highly personal character, such as expressions of feelings and thoughts, unconscious experience, or sexuality are thus generally off-limits for bulk collection (§ 22 BND Act). Even interests of paramount importance cannot typically justify an intrusion in the core of private life.[22]

c. Mandatory Application of the Hypothetical New data Collection Rule

The German constitutional court's "*criterion of hypothetical new data collection*" constitutes another interesting example of how some of the more abstract data protection standards can be applied to concrete situations of intelligence practice. Accordingly, when assessing the legitimacy of using data for different purposes than those originally intended, the constitutional court based its ruling around how the weight of the change in purpose of the data sharing compares to the original data collection purpose. The court noted that the new purpose for data collection would also have to be permissible under constitutional law using similar means.[23]

---

20 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 193. https://data.guardint.org/en/entity/neb3eo8hl9h?page=52

21 The BND Act now offers increased protections to communications of certain professional groups such as journalists, lawyers or priests (§ 21 BND Act). However, when facts justify the assumption that a person from one of these three groups is the perpetrator or participant in certain criminal offenses, the targeted data collection (i.e. the use of search terms related to that person) is allowed. The same is the case if the data collection is necessary to prevent serious threats to life, limb or freedom of a person and a number of other permissible aims listed in section 2 of § 21 BND Act.

22 Given that technical parameters and search terms are insufficient means to determine whether the core sphere of private life is affected, the BND is required to conduct manual assessments and must delete pertinent data immediately. In unclear cases, the Independent Control Council (see section 4) must scrutinize whether the data may be processed further (§ 22 (3) BND Act).
See in: Federal Government. "Explanatory Statement of the draft BND Act". November 25, 2020, p. 74. https://www.bundesregierung.de/resource/blob/976020/1823782/3074e1071c01c425e00d2ae81ffa907e/2020-12-01-refe-bnd-gesetzentwurf-data.pdf.

23 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 216. https://data.guardint.org/en/entity/neb3eo8hl9h?page=68

d. Volume Limitation

The amended BND Act limits the amount of data the BND may collect to a maximum of 30 percent of the transmission capacity of all globally existing telecommunications networks (§ 19 (8) BND Act).[24] This is in response to the German constitutional court's general clarification that the main goal of the requirements in the principle of proportionality is to limit telecommunications surveillance to a narrow enough set of criteria. The German constitution, the court clarified, "does not allow for "global and sweeping surveillance," even for foreign intelligence.[25]

Whether this new volume limitation in the BND Act will cause an actual decrease in bulk collection has been subject to debate during the policymaking process. Eco, an international business association of internet service providers, argued—in their official commentary on the draft law—that "30 percent of all global telecommunications networks" does not constitute a verifiable limit. They explained that about 70,000 communications networks participate in international data traffic, which would mean that targeting roughly 20,000 networks would be permissible under the BND Act. In Germany alone, about 1,250 carriers are linked to the internet. The legal volume limitation would consequently permit data collection up to 16 times the entire data traffic amount in Germany. A small number of large telecommunication networks have a dominant share in overall data traffic, with the 10 largest providers typically carrying about 95 percent of all data transmissions and the 25 largest networks transmitting roughly 99 percent.[26] Thus, whether this volume limitation rule qualifies as a sufficient limit of bulk interception is questionable. Taking into account that the BND's technical and financial capacities will hardly suffice to get close to such an abstract data collection cap, plus recalling that the BND may collect data in bulk as part of its suitability tests, the defined legal maximum of 30 percent is unlikely to have much practical value.

Compared to the U.S. Executive Order 12333—which allows the U.S. government to conduct bulk collection of foreign intelligence without judicial

24 Whether this volume limitation of 30 percent applies to suitability tests that the BND can conduct according to § 24 of the BND Act is not further specified in the BND Act and we suspect it does not.

25 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 168. https://data.guardint.org/en/entity/neb3eo8hl9h?page=46

26 eco. Official Statement on the draft BND Act. February 18, 2021, p. 3. https://www.bundestag.de/resource/blob/823354/a8060be2f61786ee68a7baec7be153e9/A-Drs-19-4-731-E-data.pdf

oversight and volume limitation, the specific provisions in the BND Act protecting the right to privacy of correspondence, posts and telecommunications (Art. 10 of the Basic Law), press freedom (Art. 5 of the Basic Law), as well as protecting professional communications and the core of private life of foreigners from German bulk collection represent significant progress.

Currently, Section 2 of U.S. Presidential Policy Directive 28 (PPD-28) provides some limitations on bulk surveillance and protections for non-U.S. persons' data—it requires intelligence agencies to only use signals intelligence (SIGINT) collected in bulk for six designated purposes. The permitted categories are for the purposes of detecting and countering threats from or regarding: espionage; terrorism; weapons of mass destruction; cybersecurity; U.S. or allied Armed Forces; and (6) transnational criminal acts.[27] These categories are relatively broad, and they only govern the use of data collected in bulk, rather than limiting the collection itself. Accordingly, intelligence agencies can still engage in broad bulk collection for any foreign intelligence purpose, and PPD-28 only restricts how the government may use the data once it is in government databases, allowing room for overcollection and potential misuse of data. Notably, PPD-28 merely speaks to the privacy interests of non-nationals rather than privacy rights.

As an initial reform to respond to the CJEU, the Open Technology Institute (OTI) has recommended that the U.S. government build upon PPD-28 by applying the six-category use limits for bulk data to cover the purposes for bulk collection, barring any other type of bulk collection—and that such limits should be codified into law.[28] Further, the U.S. government should adopt binding rules to ensure that even within these six categories, bulk collection is only conducted when it meets the standards of necessity and proportionality under international human rights law. When a government or entity is considering instituting policies or practices that would restrict key rights, the necessity principle requires the actor to ensure that the restriction on fundamental rights is necessary and meets a "pressing social need." Proportionality ensures that any advantages conferred by restrictions on fundamental rights are not outweighed by potential disadvantages.[29] In the longer term, Congress should consider enacting a law

27 PPD-28 at Section 2, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

28 Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman, and Spandana Singh, "Strengthening Surveillance Safeguards After Schrems II: A Roadmap for Reform," New America's Open Technology Institute, April 7, 2021, https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/

29 *See* Human Rights Committee general comment No. 31 (2004), on the nature of the general legal obligation imposed on States parties to the Covenant, https://docstore.ohchr.org/

that applies these purpose limitations (or other purpose limitations that meet the international standards of necessity and proportionality) to all intelligence.

e. Stronger Safeguards for Data Transfers as Part of Transnational Intelligence Cooperation

In *Centrum för Rättvisa v. Sweden*, the European Court of Human Rights formulated four essential safeguards that should govern the sharing of information from bulk collection with foreign partner services. First, the circumstances in which the data can be transferred must be clearly laid out in domestic law. Second, the state transferring the data must ensure the state receiving the data has adequate safeguards in place that prevent "abuse and disproportionate interference." Specifically, the receiving state must ensure secure storage of the data and restrict its onward disclosure. Third, the court noted that heightened safeguards will be necessary when clearly dealing with the transfer of materials that require confidentiality—such as confidential journalistic materials. Fourth, the court stated that the transfer of materials to foreign intelligence partners should be subject to independent control.[30]

These four safeguards can be fleshed out further—as indicated above with regard to the new provisions in the BND Act protecting professional communications data from disproportionate bulk collection. Regarding the first such safeguard, the amended BND Act provides several comprehensive provisions around how data transfers in the course of SIGINT cooperation agreements may take place. More specifically, bulk data sharing requires written agreements, so-called memorandums of understanding (*Absichtserklärung*), that specify the purposes of bulk data exchanges. § 31 section 3 of the amended BND Act lists three permissible operational purposes for transnational cooperation with other intelligence services: the early detection of severe threats, the protection of foreign and security interests of the Federal Republic of Germany, and if the operations of the BND would otherwise be made very difficult or impossible.

In practice, this means that the BND must negotiate agreements with foreign services about the exchange of search terms for bulk interception, as

30 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 276. https://data.guardint.org/en/entity/neb3eo8hl9h?page=74

well as the automated transfer of unevaluated bulk data.[31] For data collection based on search terms, the BND can receive and use search terms determined by foreign intelligence services to scan data traffic and forward the relevant hits automatically to the foreign services. Conversely, the BND may also transmit its own search terms to foreign agencies, who then feed them in their operational data collection systems (assisted data collection pursuant § 28 BND Act).

The new obligations for how the BND has to handle seeking assurances from foreign partners when sharing bulk data provides an example of safeguards that could be included in future U.S.-EU cross-border data transfer agreements. More specifically, the BND Act lists eight binding assurances that the BND needs to negotiate with its partner services. For example, the foreign partner service needs to agree to delete data related to German citizens and organizations, protected groups, and the core of private life.[32]

These new explicit requirements to seek binding assurances from foreign partner services came in response to the German constitutional court's decision declaring Germany's previous foreign intelligence legislation partly unconstitutional. The court stipulated that to ensure an adequate level of data protection in recipient countries, particular consideration is required to determine whether limits on the use of data—as well as requirements around control and data security—are generally observed.[33]

The Dutch intelligence legislation provides an additional example for those engaged in U.S.-EU negotiations. This legislation requires comprehensive risk assessments with the help of "weighting notes" on the basis of the following five criteria:

31 Note: The MoUs that the BND concludes with partner services must be approved by the Federal Chancellery if it involves foreign public bodies from EU or NATO member states (§ 31 (7) BND Act). All other cooperation agreements must be approved by the head of the Federal Chancellery and the parliamentary oversight committee must be informed about the conclusion of new MoUs. If the MoU entails sharing unevaluated bulk data automatically, it requires the head of the BND to sign off (§33 (3) BND Act).

32 In addition, § 31 (4) BND Act, our informal translation, obliges the foreign intelligence service to seek the following assurances: that purpose limitations are adhered to and data is only shared with third parties if the BND agrees; that data use is compatible with fundamental principles of the rule of law and, in particular, that data may not be used for political persecution or for inhuman or degrading punishment or treatment or for the suppression of the political opposition or certain ethnic groups; that the BND may receive, upon its request, information about the data processing by a foreign service; that data will be deleted upon request of the BND.

33 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 236. https://data.guardint.org/en/entity/neb3eo8hl9h?page=61

- The democratic embedding of the intelligence and security services in the country concerned;
- The respect for human rights in the country concerned;
- The professionalism and reliability of the service concerned;
- The legal powers and capabilities of the service in the country concerned; and
- The level of data protection maintained by the service concerned.[34]

These weighting notes can be reviewed by the independent oversight body The Review Committee on the Intelligence and Security Services (CTIVD) and must be regularly kept up to date.

f. Prior Authorization of Search Terms Used for Automated Transfer of Data in the Context of Intelligence Cooperation

The use of partner services' search terms and subsequent data transfers is another important practice area that requires safeguards for protecting data from unproportionate government access in the context of intelligence cooperation. Here, the German constitutional court ruled that the Bundestag must create related rules to ensure the Federal Intelligence Service's responsibility regarding the rights of the data it collects and processes. Specifically, the court stated that there must be a thorough assessment of the search terms determined by the foreign partner, and the resulting matches. These both must be checked to identify—where possible—data about persons or situations where special protection is needed, such as with whistleblowers. The court also pointed to the need for safeguards for fundamental rights.

This ruling also discussed safeguards for persons whose work requires confidentiality protection under law, such as lawyers and journalists. These include rules around filtering search terms that are meant to intercept telecommunications of these types of individuals, as well as manual screenings. The foreign partner may also be required to "plausibly demonstrate" why it wants to use such search parameters. Additionally, before the Federal Intelligence Service can provide automated sharing with a foreign partner, it must verify the search terms used in order to determine if data can be attributed to persons that require additional protection. In some cases, they may

34 Eijkman, Quirine et al. "Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?". 2018, p.31. https://www.ivir.nl/pub- licaties/download/Wiv_2017.pdf; see also: Dutch Act on the Intelligence and Security Services. 2017, Articles 88–90. https://wetten.overheid.nl/BWBR0039896/2021-07-15

be required to manually screen this data. Individual decisions must also be subjected to judicial review.[35]

While the Bundestag shied away from introducing a general independent approval power for transnational data sharing in response to these findings, it established an ex ante oversight power if the BND wants to share personal data related to communications of protected professions.[36] Accordingly, the BND may share personal data from communications of protected professions, for example journalists, only if the judicial control body approves the transfer. It must weigh the foreigners' interests in protected confidential communications against the legitimate operational aims of the BND in its lawfulness test before data is transferred. Such a transfer of a lawyer's personal data would be allowed if the evidence justifies the suspicion that the person in question may be the perpetrator or participant of a crime or if the transfer is necessary to prevent dangers to certain legal interests (§ 29 (8) in connection with § 30 (9) BND Act). In case of imminent danger, a preliminary approval by one member of the oversight body suffices to permit the data transfer. If the decision is later revoked, the BND shall request the deletion of the shared data (§ 29 (8) sentence 5 BND Act).

Likewise, throughout the *Schrems II* decision, the CJEU referred to the U.S. intelligence agencies' "mass processing" of EU citizens' personal data as an infringement upon the General Data Protection Regulation (GDPR), seeming to suggest that use limitations could be helpful in mitigating these concerns. The U.S. government should therefore adopt stronger and more transparent limits on how collected information—regardless of the subject's nationality—may be used. For example, information collected under Section 702 should only be permitted for use in connection with the approved foreign intelligence purpose (the certification approved by the FISA court) for which it was collected.

B. Insufficient Protection of Non-Nationals' Rights

1. Problem Analysis

While our personal data crosses borders and jurisdiction with nearly every click we make online, safeguards and enforceable rights are mostly organised at a national level. For example, imagine a European national based

35 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 236. https://data.guardint.org/en/entity/neb3eo8hl9h?page=67

36 BND Act. §§ 29 (8) and 30 (9) BND Act in connection with § 42 (1) number 5. https://data.guardint.org/en/entity/dwo3l04euwc

in Belgium who shares personal data with a U.S. company. In most jurisdictions in Europe and in the United States, fundamental privacy rights are dependent on territoriality and citizenship. As neither a U.S. citizen nor resident, the European data subject in Belgium therefore does not enjoy Fourth Amendment rights in the United States.

Fundamental rights should be considered as interdependent globally with regard to both the large amounts of data transfers across borders and to modern intelligence practice. Disregarding the rights of non-nationals bears the risk of rendering fundamental rights meaningless and undermining the rule of law—and even democracy as a whole. Recent jurisprudence in Europe has already pointed in such a direction. The German constitutional court found that human rights cannot be restricted territorially and that German authorities are bound by the basic law no matter where they operate.[37] With this, the court gave "recognition to the expanding sphere of action of German state authority."[38] Similarly, in *Schrems II*, the CJEU demanded equivalent and enforceable rights for European citizens in the United States.[39]

Additionally, as illustrated by the impact of the *Schrems II* judgement, the absence of privacy rights for non-nationals in the context of national security can impede the free flow of data across borders. If such impasses are not resolved, a worst case scenario would be a fragmented (or even "sovereignized") internet. But even now, insufficient privacy protections and lacking legal certainty constitute a major obstacle for EU and U.S. economies.

It is important to reconceptualize privacy rights. Currently they are too dependent on either nationality or residency even though personal data is de facto rarely confined by national borders. In order to prevent further impasses, it is important to enact strong and reasonable safeguards that both allow data exchange with trust that respects fundamental rights, and at the same time, do justice to the high sensitivity of intelligence work.

37 The German BVerfG stipulated that Article 10 of the German Basic Law (Grundgesetz) can be regarded as universal human rights and therefore demanded the respect of these rights by the government in all its actions – be it domestically or abroad. However, notification duties the German government has towards its own citizens are practically suspended for foreigners abroad. Arguably, this means that judicial redress becomes close to impossible for foreign citizens.

38 Irion, Kristina. "Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law". July 24, 2020. https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/

39 Court of Justice of the European Union. Schrems II Judgement. July 26, 2020, recital 91. https://data.guardint.org/en/entity/k4ae1290jz?page=26

2. Roadmap toward Positive Change

a. Redress

In order for rights to be effective, they need to be enforceable. In *Schrems II*, the CJEU ruled that "the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law." Therefore, it ruled, legislation that does not provide individuals the ability to pursue legal remedies—either for access to personal data about the person or to rectify or erase the data—does not "respect the essence of the fundamental right to effective judicial protection."[40]

The right to redress is one of the most contentiously discussed issues emerging from the *Schrems II* judgement, as it is most difficult to reform in the United States. There, the Fourth Amendment to the Constitution, which confers privacy rights, applies to citizens or residents only. Further, when the government plans to introduce evidence against an individual that was obtained under FISA, the government must notify the "aggrieved person" so that they may challenge the surveillance. Aggrieved citizens or residents have the ability to challenge the surveillance or sue the government in a separate action—amounting to "redress," as they have legal remedies available to them. By contrast, EO 12333 sets no mechanisms for redress.

Targets of U.S. surveillance under FISA Section 702 and EO 12333, including EU citizens, therefore, lack a mechanism through which they can seek redress in U.S. courts. Granting "enforceable data subject rights and legal remedies" to European citizens is a central demand of the CJEU in *Schrems II*.[41] In particular, the CJEU noted that FISA Section 702 and EO 12333 do not grant surveilled persons "actionable" rights of redress before "an independent and impartial court."

Again, it remains questionable whether many EU member states themselves even comply with the provisions demanded by the CJEU. The Swedish Signals Intelligence Act, for instance, offers effective redress against misuse of data by intelligence actors, regardless of nationality and residence of the concerned individual.[42] This is not the case everywhere in Europe. In Germany,

40 Court of Justice of the European Union. Schrems II Judgement. July 26, 2020, recital 187. https://data.guardint.org/en/entity/k4ae1290jz?page=40

41 Court of Justice of the European Union. Schrems II Judgement. July 26, 2020, recital 91. https://data.guardint.org/en/entity/k4ae1290jz?page=26

42 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 61 and 173. https://data.guardint.org/en/entity/wdwrxl9tv6f

unless one's communication data is protected by virtue of its professional characterization (e.g., for journalists) or by virtue of one's identity as a citizen of Germany or the European Union, the new SIGINT framework offers little explicit protection, let alone redress options.[43] There is, moreover, the expectation on the U.S. side that such rights need to be reciprocal, as experts, such as Peter Swire have stated : "It's common sense to have a reciprocal approach (i.e., to give U.S. citizens the right to appeal when European national security agencies access their data)."[44]

As OTI has previously written, legislation will be needed to fully meet the redress standard set.[45] This is because the high bar that the CJEU set forth in their decision requires an independent tribunal that has a fact-finding ability, and which is available to non-U.S. nationals. No such entity currently exists, and one would need to be created by statute. As other advocates have noted, legislation would also be needed to implement any approach that involves enabling complainants to establish standing—the constitutional requirement that litigants show they have been harmed by a law or practice in order to challenge it in court.

There are major obstacles to achieving the ability for redress that the CJEU called for. The first is standing, or the ability of an individual to bring a claim in some sort of tribunal to challenge the use of surveillance powers where any decision will have binding force upon the government. Standing has been difficult to achieve, even for U.S. nationals in the United States, due to secrecy surrounding the use of surveillance mechanisms, including the government's use of the State Secrets Doctrine (SSD).[46] This doctrine–which has been described as rooted in either the U.S. Constitution's commander-in-chief language, or its concept of separation of powers–allows the government to refuse to turn over or introduce evidence that it claims would

43 Vieth-Ditlmann, Kilian and Thorsten Wetzling. "Caught in the Act?: An analysis of Germany's new SIGINT reform." 2021. https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform.pdf

44 Scott, Mark. "POLITICO Digital Bridge: Rotten Apple? - Trump fallout - Digital tax standoff". *Politico.* May 6, 2021. https://www.politico.eu/newsletter/digital-bridge/politico-digital-bridge-rotten-apple-trump-fallout-digital-tax-standoff/

45 Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman, and Spandana Singh, "Strengthening Surveillance Safeguards After Schrems II: A Roadmap for Reform," New America's Open Technology Institute, April 7, 2021, https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/.

46 Goitein, Elizabeth and Schwarz, Frederick A.O. Jr., Congress Must Stop Abuses of State Secrets Privilege, Brennan Center, December 14, 2009, https://www.brennancenter.org/our-work/research-reports/congress-must-stop-abuses-secrets-privilege.

harm national security if released.[47] The U.S. government has traditionally been given wide deference by U.S. courts in its use of the SSD.[48] Without access to the evidence necessary to establish that an individual has been surveilled, many claimants struggle to establish standing.

The recent *Wikimedia Foundation v. National Security Agency* case offers an example of how a plaintiff established standing in a surveillance-related case.[49] There, Wikimedia Foundation argued that NSA's "Upstream" surveillance program necessarily captures some of the foundation's international communications, and is therefore a violation of free-speech rights and its Fourth Amendment rights against unreasonable search and seizure.[50] (Details of NSA's Upstream program are classified, but it collects data from the internet's backbone, through the transmissions over high-speed cables that carry electronic communications into and out of the United States.) Even though the Fourth Circuit ultimately dismissed Wikimedia's challenge to Upstream surveillance, Wikimedia won on the issue of standing. This meaningful win showed that it may be possible for plaintiffs to establish standing (in particular, show "actual injury") by arguing that the nature of a particular surveillance technique in itself means the government must have collected their communications.[51]

Unfortunately, another recent case may make it more difficult for individuals to bring claims alleging privacy harms in U.S. courts, and for Congress to resolve this issue. In the 2021 *TransUnion v. Ramirez* decision, the Supreme Court further narrowed the threshold for legal standing in federal courts by ruling that "an asserted risk of future harm" is not sufficiently concrete to support standing in federal court, and that Congress's ability to establish an injury in fact through law is limited.[52] Ultimately, the decision means that even when a legal right is created through a statute, the judiciary holds the

47 Lyons, Carrie Newton. "The State Secrets Privilege: Expanding its Scope through Government Misuse." 2007. https://law.lclark.edu/live/files/9577-lcb111lyonspdf.

48 Ibid.

49 Wikimedia Foundation, et al. v. National Security Agency, et al., No. 20-1191 (4th Cir. 2021).

50 Ibid.

51 Wikimedia Foundation, et al. v. National Security Agency, et al. (2021); Alex Joel and Francesca Oliveira, "Redress: What is the Problem?," European Law Blog, Sept. 28, 2021, https://europeanlawblog.eu/2021/09/28/redress-what-is-the-problem/.

52 Donohue, Meaghan. "TransUnion v. Ramirez: Why state enforcement will be central to the success of a future federal privacy law." Techpolicy Press. July 28, 2021, https://techpolicy.press/transunion-v-ramirez-why-state-enforcement-will-be-central-to-the-success-of-a-future-federal-privacy-law/ ; Alex Joel and Francesca Oliveira, "Redress: What is the Problem?," European Law Blog, Sept. 28, 2021, https://europeanlawblog.eu/2021/09/28/redress-what-is-the-problem/.

ultimate authority to determine when a violation of that right has resulted in an injury.[53]

b. Notification Duties

Formal notification after personal data processing plays a crucial role in ensuring the right to an effective remedy - for two reasons. First, standing in court is in many cases dependent on proof that surveillance of the applicant has happened. This proof is difficult to gather without notice. Second, data subjects that are not even aware that they are being surveilled can not seek remedy. In this way, notice is one of the threshold problems to redress. In some cases, certain requirements, logistical and safety issues make it difficult to inform non-nationals and non-residents that they are being surveilled. In other cases, secrecy regulations make it difficult for subjects to know they are a surveillance target in the first place.

In Germany, where the constitutional court accorded equivalent rights to non-nationals and non-residents, the court itself acknowledged that notification of the data subject is often impossible when non-nationals or non-residents are affected by surveillance. However, secrecy requirements and logistical difficulties in reaching data subjects that are situated outside of a country's jurisdiction are just two of the reasons why notice for non-nationals is often problematic. Additionally, notifying non-nationals could—depending on the context—endanger the data subjects themselves and, for instance, render them suspect to secret services or law enforcement in their country. For example, if the German BND would notify a Syrian citizen that they have been subject to surveillance by Germany, this communication may come to the attention of the local security services and could result in considerable danger for the person involved. In some instances omitting subsequent notification of the data subject is therefore in the interest of the data subject in question.

In the United States, even U.S. citizens often can not establish standing in court because they cannot prove that they are affected by the surveillance measures, due to lack of notification.U.S. intelligence law does not provide for notice in many situations. Under FISA, the U.S. government must provide

53 Donohue, Meaghan. "TransUnion v. Ramirez: Why state enforcement will be central to the success of a future federal privacy law". *Techpolicy Press*. July 28, 2021. https://techpolicy.press/transunion-v-ramirez-why-state-enforcement-will-be-central-to-the-success-of-a-future-federal-privacy-law/; Alex Joel and Francesca Oliveira, "Redress: What is the Problem?," European Law Blog, Sept. 28, 2021, https://europeanlawblog.eu/2021/09/28/redress-what-is-the-problem/.

advanced notice to a criminal defendant if they intend to use evidence collected under Section 702 at trial or other proceedings.[54] The Supreme Court further ruled in *Clapper v. Amnesty International* that "the government... must provide advance notice of its intent" if they intend to "use or disclose information obtained or derived" from Section 702.[55]

While by law this notice must be provided, in practice criminal defendants rarely receive notice that they have been subject to Section 702 surveillance. In 2015, ACLU's Patrick Toomey expressed dismay about why this continues to be the case, noting the Department of Justice's notice policy—and interpretation of FISA's requirements—are kept secret. He noted that, "because of this secrecy, the public, courts, and criminal defendants are unable to determine whether DOJ's current view of its duty to give notice is even remotely defensible."[56]

The ability to receive notice for other intelligence gathering authorities is even worse. The Patriot Act includes no provisions for notice, and the government has not provided any. However, resourceful libraries and other organizations have taken advantage of the gag orders that usually accompany Patriot Act orders to provide "canaries" in the form of statements that they had *not* received such an order.[57] Finally, under Executive Order 12333, no administration has ever publicly disclosed what they view their obligations to be when it comes to notification.

In cases where the court's jurisdiction is not limited by whether the subject of surveillance has notice (unlike the United States), this barrier becomes much less of an issue. For example, the European Court of Human Rights has held on several occasions that notification duties are not necessary "where the courts' jurisdiction does not depend on notification to the interception

54 50 U.S. Code § 1806

55 Clapper v. Amnesty International. 568 U.S. 398 (2013). https://www.supremecourt.gov/opinions/12pdf/11-1025_ihdj.pdf

56 Toomey, Patrick C. "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?" *Just Security.* December 11, 2015. https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/

57 Electronic Frontier Foundation, Warrant Canary Frequently Asked Questions, April 10, 2014, https://www.eff.org/deeplinks/2014/04/warrant-canary-faq.

subject that there has been an interception of his or her communications."[58] Similarly, the court highlighted that the British Investigatory Powers Tribunal (IPT), which has comprehensive jurisdiction over British intelligence activities, can examine any complaints about illegal interceptions regardless of notifications to the data subject.[59]

c. Compensatory Approach and Effective Review

Even with equivalent rights and the theoretical possibility of having standing in court, legal protection for foreigners may remain limited in actual practice. Secrecy and security concerns (including for the data subject) limit the extent to which non-nationals' rights can be enforced. As mentioned earlier, non-nationals may not, for example, receive the same types of notifications about past surveillance of their communications' data that nationals do—at least in some jurisdictions, such as Germany. In turn, this is a notable disadvantage when it comes to a non-national's attempt to seek effective remedy in courts. To compensate for the "virtual absence of safeguards commonly guaranteed (to non-nationals) under the rule of law" and the "gap in legal protection," the German constitutional court has requested that specific safeguards are respected and has demanded reinforced and comprehensive judicial and administrative oversight over the BND's treatment of non-national communications data.[60] The new German Federal Foreign Intelligence Law now places strategic surveillance of non-nationals under quasi-judicial oversight within the newly created *Unabhängiger Kontrollrat* (Independent Control Council).

In light of the reduced possibilities for rights enforcements and remedy for non-nationals, involving adversarial representatives that specifically argue in the interests of the affected group could provide another layer of protection.[61]

58 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 271. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=72 and European Court of Human Rights. Big Brother Watch and Others v. The United Kingdom. May 25, 2021, recital 358 https://data.guardint.org/en/entity/8bxe5z9q3ar?searchTerm=notification&page=109 and previously other case law by the ECHR, too: *Roman Zakharov*, § 234 and *Kennedy*, cited above, § 167

59 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 199. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=53

60 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 268-272. https://data.guardint.org/en/entity/neb3eo8hl9h?page=70

61 See also the section on "ineffective review mechanisms and the call for end-to-end oversight further below.

d. Possible International Instrument

Since the *Schrems II* decision, experts have pondered about new opportunities for a "more sustainable kind of transatlantic cooperation on security and civil liberties, in which technology and intelligence sharing goes together with real cross-national protections for civil liberties."[62]

International cooperation between national oversight bodies could be a novel mechanism alleviating limited redress possibilities (among other issues). Such cooperation can take many forms and will require mutually acceptable regulations on effective redress. This could go in the direction of aligning standards to ensure an equal standard of privacy for citizens of participating states, as proposed by the Parliamentary Assembly of the Council of Europe with its "Intelligence Codex" in 2015.[63] More extensive cooperation in the field of intelligence oversight—for instance in the form of an international authority—could be used to strengthen the de facto privacy rights of non-nationals facing limited options for effective redress. The draft "Legal Instrument on Government-led Surveillance and Privacy" by the UN Special Rapporteur on Privacy Joe Cannataci also proposed, in 2018, that an international authority be put in place to oversee privacy matters between signatory countries.[64] More recently, the Global Privacy Assembly encouraged governments and international organisations to develop "multilateral instruments ensuring adherence to key data protection and privacy principles in relation to government access to personal data."[65]

Admittedly, such instruments are unlikely to be implemented on a global level. However, an agreement could potentially be reached at a smaller scale

62 Farrell, Henry and Abraham L. Newman. "Schrems II Offers an Opportunity - If the U.S. Wants to Take It". *Lawfare*. July 28, 2020. https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it

63 Parliamentary Assembly of the Council of Europe. "Mass Surveillance Endangers Human Rights and Does Not Prevent Terrorist Attacks, Says Council of Europe". 2015. https://ccdcoe.org/incyder-articles/mass-surveillance-endangers-human-rights-and-does-not-prevent-terrorist-attacks-says-council-of-europe/

64 "States shall establish an International Data Access Authority with the purpose of protecting personal data, privacy, freedom of expression and other fundamental human rights while facilitating the timely exchange of personal data across borders as may be required for the legitimate purposes of law enforcement agencies, intelligence and security services." In: Cannataci, Joseph A. "Draft Legal Instrument on Government-led Surveillance and Privacy. Including the Explanatory Memorandum." 2018. https://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf

65 Global Privacy Assembly. "Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes". October 2020. https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf

among certain countries that share the same values, perhaps in the spirit of an "alliance of democracies," as Henry Farrell and Abraham L. Newman have proposed.[66] Such an alliance could prove helpful to foster the respect of civil rights and liberties as the backbone of democracies, especially vis-à-vis authoritarian countries such as China and Russia.[67] In a recent study for the European Parliament requested by the Committee on Civil Liberties, Justice and Home Affairs (LIBE), for instance, Ian Brown and Douwe Korff proposed a "minilateral treaty" on intelligence activities between the EU and the Five Eyes countries including "clear rules on the states concerned not surreptitiously spying on each other, with transparent arrangements for mutual assistance, subject to crucial rule of law and human rights safeguards and openness about practice."[68]

C. Ineffective Review Mechanisms and the Call for End-to-End Oversight

1. Problem Analysis

Much of recent European jurisprudence—not just in the CJEU *Schrems II* case, but also in other judicial proceedings at the European Court of Human Rights and in the highest national courts—have focused on bulk collection and its democratic oversight.[69] Some European parliaments recently amended, or are about to introduce, legislative changes to the codified mandates of intelligence services, as well as the laws and regulations on

66 Farrell, Henry and Abraham L. Newman. "Schrems II Offers an Opportunity - If the U.S. Wants to Take It". *Lawfare*. July 28, 2020. https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it

67 Wetzling, Thorsten and Charlotte Dietrich. "Wanted: better safeguards for intelligence in an interconnected world". *about:intel*. October 15, 2020. https://aboutintel.eu/common-intelligence-standards/

68 Brown, Ian and Douwe Korff. "Exchanges of Personal Data After the Schrems II Judgment". *IPOL - Policy Department for Citizens' Rights and Constitutional Affairs.* July, 2020, p.10. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

69 This includes the two recent Grand Chamber decisions of the European Court of Human Rights, namely Centrum för rättvisa v. Sweden (no. 35252/08) and Big Brother Watch and Others v. United Kingdom (nos. 58170/13, 62322/14 and 24960/15). In addition, one can point to CJEU jurisprudence on national data retention regulations (Case C-623/17 and the joined Cases C-511/18, C-512/18 and C-520/18), which attracted significant commentary and attention. Moreover, one can point to landmark judgments on SIGINT practice, legislation, and oversight by national courts, such as the High Court and the Supreme Court in the United Kingdom, the Constitutional Court and the Highest Administrative Court in Germany. Of interest, for comparative legal analysis are also the landmark decisions of the Constitutional Courts of Austria and, further afield but no less interesting, of South Africa.

the institutional design and mandate of oversight institutions.[70] Meanwhile, some intelligence services, such as the U.K.'s GCHQ, have recently increased transparency regarding their use of artificial intelligence and their respective data ethics frameworks.[71] In so doing, they acknowledged that legal frameworks and oversight practice need to be further aligned with this development.

It is of utmost importance to provide effective oversight and accountability for a highly complex and big data-driven intelligence collection process that interferes—at several stages—with fundamental rights. Oversight provides a much-needed check on the executive branch, and also adds legitimacy to its use of investigatory powers, ideally preventing executive overreach and establishing public trust in the intelligence process. In order to achieve these goals, oversight must go far beyond rubber-stamp authorization and weak ex-post review mechanisms—oversight must be driven by independent and rigorous fact-checkers that have substantial resources, sufficient decision-making, and enforcement powers.

Before delving into how the oversight and accountability process can be strengthened, it is useful to discuss some common points of friction regarding oversight—both in the United States and across Europe—which largely show that oversight and accountability are somewhat elusive goals, and are a constant work in progress.[72]

70 This concerns, for example, Germany, France, Norway and Sweden but there are also frequent ongoing discussions about necessary reforms to U.S. surveillance legislation. For a recent discussion, see Bradford Franklin et al. "Strengthening Surveillance Safeguards after Schrems II: A roadmap for Reform." *New America's Open Technology Institute.* 2021. newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/2; Kerry, Cameron F. "The Oracle at Luxembourg: The European Court of Justice judges the world on surveillance and privacy. Brookings Report. 2021. https://www.privacysecurityacademy.com/wp-content/uploads/2021/03/The-oracle-at-Luxembourg_-The-EU-Court-of-Justice-judges-the-world-on-surveillance-and-privacy.pdf

71 Murray, Daragh and Peter Fussey. "GCHQ's ethical approach to AI: an initial human rights-based response." *about:intel.* March 5, 2021. https://aboutintel.eu/qchq-ethics-ai/ and GCHQ. "Pioneering a new national security. The ethics of artificial intelligence." 2021. https://www.gchq.gov.uk/files/GCHQAIPaper.pdf

72 Interestingly, as noticed by the European Court of Human Rights, "at least seven Contracting States (being Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways". European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 131. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=40 Spain, Italy, Belgium and Denmark have sizeable intelligence communities but they are not mentioned in this list.

a. The French Council of State on the French Intelligence Oversight Body CNCTR

In response to the CJEU's influential October 2020, where it ruled that France's surveillance laws did not safeguard fundamental rights and freedoms, the French Council of State laid out in April 2021 how the CJEU's judgment—amongst other interpretations—ought to be translated into concrete legislative reform in France.[73] More specifically, as discussed by Arthur Messaud and Noémie Levain, "[it] found that [the French] review mechanism is too permissive compared to what the CJEU has required."[74] Theodore Christakis elaborated that the French Council of State gave the French Parliament "six months [...] to introduce all new mechanisms, procedures and safeguards," including a requirement that France change its surveillance law to provide the National Commission for the Control of Intelligence Techniques (CNCTR), an independent oversight body, with authority to render binding opinions related to intelligence data.[75] There might be additional room for oversight improvement, though—as Arthur Messaud and Noémie Levain have suggested—because CNCTR does not have access to information that French intelligence services collect from foreign partners.[76] Provided that analysis is correct, then this appears to stand in conflict with the European Court of Human Rights' findings in *Centrum för Rättvisa v. Sweden* about minimal procedural and legislative safeguards for intelligence sharing.[77]

73 Council of State. French Data Network and Others. April 2021. https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043411127

74 Messaud, Arthur and Noémie Levain. "CJEU rulings v. French intelligence legislation". *about:intel*. May 14, 2021. https://aboutintel.eu/cjeu-french-intelligence-legislation/

75 "For instance, the Council of State stressed that France needs to change its surveillance law so as to render binding the opinions given by the National Commission for the Control of Intelligence Techniques (CNCTR), an independent oversight body, with regard to the use of data that is retained for intelligence purposes. Similarly, France will need to take stock of the 2 March 2021 [CJEU's] *Prokuratuur* judgment especially in view of the requirement that competent law enforcement authorities' access to retained data must always be subject to a prior review carried out either by a court or by an entirely independent administrative body." Christakis, Theodore. "French Council of State discovers the 'philosopher's stone' of data retention." *about:intel*. April 23, 2021. https://aboutintel.eu/france-council-of-state-ruling/

76 "Lastly, where French intelligence services collect information from foreign services, such an access is never subject to CNCTR's review. This has been a recurring complaint from the CNCTR (and us) for years. Both the Government and the Conseil d'État have refused to address it (in its recent ruling, the Conseil d'État acted as if we never raised the issue)." Messaud, Arthur and Noémie Levain. "CJEU rulings v. French intelligence legislation". *about:intel*. May 14, 2021. https://aboutintel.eu/cjeu-french-intelligence-legislation/

77 Consider also the pertinent findings (discussed above) of the German Constitutional Court on prior authorization of foreign search terms used for automated transfer of data in the context of intelligence cooperation.

b. Independence of the Oversight Body

In the May 2021 European Court of Human Rights (ECtHR) Grand Chamber decision on *Centrum för Rättvisa v. Sweden*, Judge Pinto de Albuquerque wrote a concurring opinion in which he criticized the "highly politicised status of the FIC's [Sweden's Foreign Intelligence Court] members," noting that it has "never held a public hearing and its decisions are final and confidential."[78] As a result, he argued that the Swedish oversight bodies "either do not meet the requirement of sufficient independence or provide effective scrutiny, or both."[79]

c. German Constitutional Court on Insufficient Resources and Expertise in Previous German Oversight Body

In its ruling regarding the BND Act, the German constitutional court stated that people must be appointed to the oversight body as their primary occupation to ensure the oversight is "competent and professional." The court noted that it is not sufficient to have an oversight board act in an honorary capacity. It also determined that oversight bodies must be able to develop their own databases and software, in part to ensure the bodies can effectively scrutinize key components such as filtering mechanisms. [80]

d. U.S. Department of Justice Inspector General's Audit of FISA Procedures

In the United States, the recent DOJ Inspector General audit of FISA "Woods Procedures," released September 30, 2021, has also raised significant questions about oversight and accountability in the FISA process. Woods Procedures are documentation requirements that are designed to ensure FISA applications are "scrupulously accurate"—each factual assertion in the applications to the FISC must have documentary support in the FBI's files.

Of the initial sample of 29 FISA applications, the audit found more than 400 instances of non-compliance with Woods Procedures. After those initial findings, the IG conducted further review of more than 7,000 FISA applications authorized between January 2015 and March 2020 and found at least 179 instances in which the required Woods file was completely missing, damaged,

78 European Court of Human Rights. Centrum för Rättvisa v. Sweden - Concurring Opinion of Judge Pinto de Albuquerque. May 25, 2021, paragraph 9. https://data.guardint.org/en/entity/wdwrxl9tv6f?searchTerm=deceitful&page=103

79 Ibid., paragraph 23.

80 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 287f. https://data.guardint.org/en/entity/neb3eo8hl9h?searchTerm=287&page=75

or incomplete.[81] FISA experts across the board were shocked by the severity of these IG audits.[82] In fact, *Lawfare's* editor in chief Ben Wittes remarked that he "will never say again in public these applications go through a rigorous process and they are subject to intense oversight within the FBI and the Office of Intelligence in the Justice Department before it ever goes to the FISA Court."[83]

e. The FISA Court Amicus Role

In the United States, the FISA amicus operates as a key check on the secretive FISA Courts. Congress created the role of the FISA amicus through the USA FREEDOM Act in 2015 as a reform to the FISA Court (as well as the FISA Court of Review, or FISCR). Under current law, FISA Court and the FISCR judges appoint a panel of at least five independent experts with security clearances who possess expertise in privacy, civil liberties, intelligence collection, or communications technology, and then task these "amici" to participate in particular cases and advise the judges on their areas of expertise.

The current standard is that amici are included in the FISA Court process during cases involving "a novel or significant interpretation of the law," but experts have pushed for expansion of their valuable role, as the amici have been limited by the law.[84] One issue is that the "novel or significant interpretation" standard relates to the legal issues involved in the case, rather than the level of threat that the surveillance poses to privacy and civil liberties. Further, amici have inadequate access to information even in the cases in which they do participate. Finally, these special advocates are not currently able to appeal from the FISA Court to the FISCR. Advocates, academics, and the Privacy and Civil Liberties Oversight Board (PCLOB) have recommended

81 Klehm, Bryce and Rohini Kurup. "Justice Department IG Releases Audit of FISA Procedures". *Lawfare*. September 30, 2021. https://www.lawfareblog.com/justice-department-ig-releases-audit-fisa-procedures; Department of Justice Office of the Inspector General, Audit of the Federal Bureau of Investigation's Executions of Its Woods Procedures for Applications Filed With the Foreign Intelligence Surveillance Court Relating to U.S. Persons, September 2021. https://s3.documentcloud.org/documents/21072938/audit-of-the-fbis-execution-of-its-woods-procedures.pdf

82 Goitien, Elizabeth et al. "Top Experts Analyze Inspector General Report Finding Problems In FBI Surveillance". *Just Security.* April 27, 2020. https://www.justsecurity.org/69879/top-experts-analyze-inspector-general-report-finding-problems-in-fbi-surveillance/

83 Klein, Adam and Benjamin Wittes. "Adam Klein and Benjamin Wittes on FISA". *The Lawfare Podcast*. October 11, 2021, 29:05-30:00. https://shows.acast.com/lawfare/episodes/adam-klein-and-benjamin-wittes-on-fisa

84 Bradford Franklin, Sharon. "A Key Part of Surveillance Reform is Now in Jeopardy". *Slate.* May 29, 2020. https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html

rectifying these flaws and most importantly, expanding the role of the amicus to include cases relating to First Amendment issues and involving novel technologies, among others. Accordingly, during Congress's 2020 attempt at reforming Patriot Act Section 215, (known as the USA FREEDOM Act of 2020) the Senate overwhelmingly passed an amendment that would adopt these key reforms.[85] Unfortunately, these reforms were never enacted, as Congress never moved to conference the Senate and House versions of the bill amid the COVID-19 pandemic shutdown.[86] (The relevant Section 215 authorities have also not been reauthorized, and have seen an unprecedented lapse.)

2. Roadmap toward Positive Change

a. Standards for Effective Review as Observed by the European Court of Human Rights

In its May 2021 decision on the Swedish legal framework for foreign intelligence collection and oversight, the ECtHR shed light on the following safeguards that should significantly strengthen the overall quality of an intelligence accountability and oversight regime:

- Establishing and improving an adversarial process within the authorization process;
- Providing information on the selectors to allow for a genuine proportionality assessment;
- Introducing a 'double lock' system for oversight bodies;
- Endowing oversight bodies with sanctioning powers even in the context of foreign intelligence collection; and
- Providing for an independent audit of the oversight process.

Regarding the first aspect, the judgment noted that „relevant safeguards against arbitrariness" should be included in the independent ex ante authorization procedure. To achieve this, the Swedish bulk interception law requires the mandatory presence of a "privacy protection representative" at court sessions, except for in urgent cases. Additionally, it points to the role of the FISA amicus in the U.S. courts as an example—a representative such as a judge, former judge, or attorney who acts "independently and in

85 See Ibid. and Leahy, Patrick J. and Mike Lee. "Opinion: FISA Needs Reform. Our Amendment Would Do That. And Protect Constitutional Rights". *Washington Post*. May 10, 2020. https://www.washingtonpost.com/opinions/2020/05/10/fisa-needs-reform-our-amendment-would-do-that-protect-constitutional-rights/

86 Ibid.

the public interest but not in the interest of any affected private individual. He or she has access to all the case documents and may make statements."[87]

Not many other countries have taken this important state „against arbitrariness,"[88] notably the recent German intelligence reform also shied away from this. It remains less than suboptimal when judicial control bodies only hear the perspective of the intelligence service members and the executive when reviewing the lawfulness of bulk warrants. In light of the special protections for certain professional groups, for example, and recalling the inherent danger of group-think, it might be very worthwhile to include adversarial representatives into authorization proceedings to argue in the interests of affected groups, such as protected professions.[89]

In addition, the ECtHR also emphasized that any independent authorization process „implies necessity and proportionality analysis,"[90] and goes on to underscore that it might be difficult for the judicial approval body „to appreciate the proportionality aspect where only categories of selectors are specified"[91] in applications for bulk interception. For example, against this backdrop, the fact that no individual selectors of any kind must be listed in the bulk warrants[92] calls into question whether the ECtHR would be satisfied with the judicial approval process pursuant to the new BND Act.

Moreover, the ECtHR's *Centrum för Rättvisa v. Sweden* judgment also examined whether the Swedish ex post oversight body, the Foreign Intelligence Inspectorate (SIUN),[93] is adequately equipped to assess aspects of the proportionality of the interference with the rights of individuals in SIGINT activities. In so doing, it observed that SIUN conducts „numerous detailed

87 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 298. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79

88 Ibid.

89 Consider also this statement on the merit of adversarial voices: "to avoid being a rubber stamp, the process needed an adversary [...] to challenge and take the other side of anything that is presented to the FISA Court [...] anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding." In: Bradford Franklin, Sharon. "A Key Part of Surveillance Reform Is Now in Jeopardy". *Slate*. May 29, 2021. https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html

90 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79

91 Ibid., recital 301.

92 See § 23 (6) sentence 2 BND Act.

93 Statens inspektion för försvarsunderrättelseverksamheten (SIUN), http://www.siun.se/index.html

examinations of, in particular, the selectors used“ and that „it is tasked with granting the FRA access to communications bearers after verifying that the requested access corresponds to the permit issued by the Foreign Intelligence Court.“[94]

This practice is not currently on the cards in many other jurisdictions. In Germany, for example, the amended BND Act does not foresee direct access to bearers of communications for the members of the newly found Independent Control Council, nor does it foresee a similar double verification method of approved warrants. More specifically, the ability to unblock particular bearers and to grant access to specific cables or facilities after checking a warrant is a powerful control competence that has yet to see the light of day in many European countries.

Moreover, as observed by the ECtHR, if the Swedish Foreign Intelligence Inspectorate identifies undue SIGINT conduct, it can also decide—with binding effect—“that the collection must cease or that recordings or notes of collected data must be destroyed.“[95] By contrast, the amended BND Act does not specify the extent to which the newly-found complaint mechanism available to the administrative control body of the ICC (§ 52 BND Act) may also be used to sanction malfeasance.

Finally, we learned from the recent ECtHR judgement that the Swedish oversight body is also subjected to independent audits by the Swedish National Audit Office. The latter evaluates whether the oversight activities make a difference and how they could be improved.[96] This independent review of an independent oversight process is also very progressive and should be considered by other nations, too. By contrast, the newly created provision in the BND Act that calls for the evaluation of the effectiveness of the ICC‘s oversight, will be conducted by the ICC itself (§ 61 BND Act).

94 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 347-348, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=89

95 Ibid., recital 350, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=16

96 Ibid., recital 54, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=90

b. More Decisions by Security and Intelligence Services Should be Subjected to Independent Review

The CJEU's *Privacy International v. Secretary of State*[97] and *La Quadrature du Net and Others v. Premier Ministre and Others* cases offer important insights into the scope of judicial review.[98]

While the former case did not pronounce on foreign intelligence legislation specifically, it clarified that "a legislative measure [...] on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission [...] exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society."[99] Moreover, it stipulated that "national legislation governing access to traffic data and location data must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue." Finding also that "those requirements apply, a fortiori, to a legislative measure [...] on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission," one can then argue that the requirements that the CJEU formulated with respect to data retention in the *LQDN* case, should equally apply to legislative measures that compel service providers to transmit data in bulk to the security and intelligence services.

Equally interesting, the CJEU recalled in the *LQDN* case that the following categories of decisions by security and intelligence services ought to be subject to an independent court's or administrative body's jurisdiction:

- A decision giving an instruction to providers of electronic communication services to carry out general and indiscriminate retention of data (paragraph 139);

97 Court of Justice of the European Union. Privacy International v Secretary of State. October 6, 2020. https://data.guardint.org/en/entity/35ernv51jnp

98 Court of Justice of the European Union. La Quadrature du Net and Others v Premier Ministre and Others. October 6, 2020. https://data.guardint.org/en/entity/20gb4kvky39j; Court of Justice of the European Union. Privacy International v Secretary of State. October 6, 2020. https://data.guardint.org/en/entity/35ernv51jnp?page=19

99 Ibid.

- Decisions on national security grounds requiring providers of electronic communication services to retain general and indiscriminate traffic and location data (paragraph 168)
- Decisions authorising automated analysis (paragraph 179);
- The sharing of real time traffic and location data (paragraph 189); and
- National rules which authorise automated analysis (paragraph 192).

Whether these decisions are sufficiently subject to the jurisdiction of oversight bodies across Europe is a matter that requires further consultation. In part this is also addressed in Chapter Three.[100]

In the United States, the PCLOB is the primary body with oversight capability over the intelligence community and activities. Among other things, the PCLOB is tasked with continually reviewing all regulations, laws, and procedures related to counterterrorism efforts, as well as "the information sharing practices of the departments, agencies, and elements of the executive branch to determine whether or not such practices appropriately protect privacy and civil liberties and adhere to the information sharing guidelines." However, as the Congressional Research Service has noted, the PCLOB "was not vested with potent authority to obtain information relative to the execution of these responsibilities," as it does not have subpoena power, among other issues.[101]

c. End-to-End Oversight as the Way Forward

There is a greater insistence both by legal courts and oversight bodies regarding the need for a more comprehensive mandate and oversight processes to cover each phase of the *information continuum*.[102] Given that each phase of the "lifecycle of information, from how it is collected and safeguarded, to how it is shared and, ultimately, how it is used to inform real-world actions undertaken for national security or intelligence purposes"[103] entails unique risks to fundamental rights and civil liberties, it is important to establish—in

100 See, for example, the discussion in: Müller, Michael W. and Thomas Schwabenbauer. "Anforderungen der Unionsgrundrechte an Datenverarbeitungen durch nationale Sicherheits- und Strafverfolgungsbehörden". Forthcoming; Vieth-Ditlmann, Kilian and Thorsten Wetzling. "Caught in the Act?: An analysis of Germany's new SIGINT reform." 2021. https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform.pdf

101 https://sgp.fas.org/crs/misc/RL34385.pdf

102 NSIRA. "2019 Annual Report". 2020, p. 20. https://nsira-ossnr.ca/wp- content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf

103 Ibid., p.21.

legislation and in actual practice—an oversight remit that subjects the entire process to rigorous independent scrutiny. This includes the initial formulation of intelligence priorities, the authorisation process, the various stages of data processing, and the numerous data sharing and retention practices. While this may have been on the agenda for quite some time now, legislation still lags behind in many countries and practice seems to encounter significant obstacles, especially when it comes to a comprehensive independent review of the various data processing processes. Yet, this is precisely where independent review is most needed because "effective review and supervision implies binding powers where the impact on the fundamental rights is the greatest, particularly in the accessing, analysis and storage phases of processing personal data."[104]

The German constitutional court judgement on the 2016 BND Act provides a recent and insightful illustration of this pressing challenge. It found fault with Germany's intelligence oversight architecture because its design and processes were deemed insufficient to satisfy the proportionality requirement. More specifically, the BND's powers to conduct strategic surveillance measures, to share the intelligence thus obtained, and to cooperate with foreign intelligence services were not complemented by sufficiently rigorous and independent oversight. The court stipulated that "it must be guaranteed that the entire process of strategic surveillance…can comprehensively be subjected to oversight."[105] The court further specified that "an oversight body must be created that can, on its own initiative, randomly scrutinise the entire process of strategic surveillance as to its lawfulness; this concerns individual decisions, processes, the design of data processing and filtering mechanisms as well as the technical resources used for them."[106]

Similarly, the ECtHR observed in its May 2021 *Centrum för Rättvisa v. Sweden* decision that "each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority. "[107] Emphasizing

104 CTIVD and TIB. "Council of Europe Convention 108+ and oversight on national security". 2021, p. 4. https://english.ctivd.nl/latest/news/2021/02/17/index

105 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 279. German Federal Constitutional Court. BND Act Judgement. May 19, 2020. https://data.guardint.org/en/entity/neb3eo8hl9h

106 Ibid., recital 276.

107 European Court of Human Rights. Centrum för Rättvisa v. Sweden. May 25, 2021, recital 270. https://data.guardint.org/en/entity/wdwrxl9tv6f?page=72

the need for supervising bodies to be in a position to assess the *necessity* and *proportionality* of the action being taken, the ECtHR also requested that "detailed records should be kept by the intelligence services at each stage of the process."[108] The German constitutional court was even more specific on the documentation of data sharing practices. It requested that "data sharing must be documented so as to ensure independent oversight of adherence to the requirements for data sharing [...] Such documentation must also specify the statutory provision on which data sharing is based."[109]

However, aside from the need to embed this principle in primary surveillance legislation, it needs to be honoured in practice. This is where most oversight bodies in Europe, even in countries where practice is comparatively quite advanced,[110] still seem to encounter substantial and long-term challenges—both regarding expertise and aptitude, but also resources required for "data-driven intelligence oversight."[111]

The basic premise has been summarised well by Graham Smith. When "sophisticated analytical techniques such as anomaly detection and pattern analysis are brought to bear on intercepted material, particularly communications data," he observed "robust end to end oversight ought to cover these techniques as well."[112]

D. Summary

On the basis of a thorough discussion of common points of friction in national surveillance and intelligence legislation that relate to cross-border data transfers, this chapter illustrated how the more abstract safeguards referred to in the CJEU *Schrems II* judgement can be fleshed out further when read in conjunction with recent European jurisprudence on national intelligence legislation and national data retention frameworks. Analysis of these rulings indicates that much more must be done to adequately safeguard against ris-

108 Ibid.

109 German Federal Constitutional Court. BND Act Judgement. May 19, 2020, recital 228. https://data.guardint.org/en/entity/neb3eo8hl9h?page=60

110 Derix, Steven and Rik Wassens. "Toezichthouders inlichtingendiensten: 'Balans tussen nationale veiligheid en privacy raakt zoek'". July 3, 2021. https://www.nrc.nl/nieuws/2021/03/07/wij- kunnen-ons-werk-zo-niet-doen-a4034577

111 Vieth, Kilian and Thorsten Wetzling. "Data-driven Intelligence Oversight. Recommendations for a System Update". 2019. https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf

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

ks of non-compliance and fundamental rights infringements when it comes to data re-use and data transfers and the rights of non-nationals including their rights to receive notice and their right to judicial remedy. This includes taking steps such as establishing specific data protection regimes for shared data, reinforcing independent end-to-end oversight, and making the right to redress independent from notification and secrecy regulations. International agreements and instruments can further play a crucial role in strengthening civil rights and liberties in democracies.

Chapter 3

Government Access to Personal Data Held by the Private Sector

Governments can gain access to data held by the private sector in two main ways. They can compel the private sector to hand out data, either by lawful means or by coercion. Or the private sector can give the government voluntary access to data, either by selling out data sets or by offering it to the government voluntarily.

Because governments are increasingly finding this commercial data valuable and obtaining it via one or both methods, a holistic review of surveillance law must include commercial data practices and how intelligence agencies can obtain and handle that data. While we are not aware of the EU-U.S. consultations including these issues, moving forward it would be wise for policymakers to consider the connection between commercial data and intelligence in order to prevent future disputes relating to international data transfers and insufficient privacy safeguards.

A. Problem Analysis

1. Compelled Access by Lawful Means

a. Compelled Access by Intelligence Agencies in Germany[113]:

The BND can compel telecommunication providers that are subject to German jurisdiction to provide access to communications data.[114] While strategic foreign telecommunications collection as laid out in §19 BND Act applies

113 The draft of the e-evidence directive at European level (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en) has led to many important discussions about safeguards regarding compelled access by law enforcement agencies (LEAs) to data held by the private sector. For the sake of clarity, and because it exceeds the scope of this report, this section will, however, focus solely on compelled access by intelligence agencies in Germany.
For a comprehensive analysis of compelled access by law enforcement agencies from a transatlantic perspective see for example: Theodore Christakis, Fabien Terpan, EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options, *International Data Privacy Law*, Volume 11, Issue 2, April 2021, Pages 81–106, https://doi.org/10.1093/idpl/ipaa022.

114 §3,4 and 8 BND Act

to foreign communications only,[115] the collection under this provision is not limited to non-German territory. Rather, due to Germany's geographical location in the heart of Europe, routing of foreign communications actually makes up a relevant fraction of overall telecommunication traffic, even in domestic communications networks.[116] If the communications of foreign entities or individuals are processed by providers within Germany, the BND can compel them to provide access to this data. Orders need to be issued by the federal chancellery, and the telecommunications firm receives compensation for the incurred costs.[117]

According to recent European case law, compelled access is only possible if it does not exceed „the limits of what is strictly necessary."[118] Indiscriminate transmission of data by providers of electronic communication services to security and intelligence agencies cannot be considered to fall within these criteria, as the CJEU clarified in its *Privacy International v. Secretary of State* case, noting: "a legislative measure [...] on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission [...] cannot be considered to be justified, within a democratic society."[119]

The CJEU further highlighted the importance of judicial or administrative oversight in its *Quadrature du Net* ruling. The court stipulated that the following categories of decisions by security and intelligence services need to be subject to an independent court's or administrative body's jurisdiction:

115 A separate law, the Article 10 Act, regulates the interception of domestic communications. The Article 10 Act, however, also goes beyond „interception of domestic communications" in that foreign-domestic traffic, i.e. communication that involves both foreign and domestic participants, is regulated in § 5 of the Art. 10 Act. For more information on the Article 10 Act and recent reform attempts, see e.g. Wetzling, Thorsten. "The key to intelligence reform in Germany: Strengthening the G 10-Commission's role to authorise strategic surveillance". https://www.stiftung-nv.de/sites/default/files/snv_g10.pdf; Vieth, Kilian and Charlotte Dietrich. "New hacking powers for German intelligence agencies". October 27, 2020. https://aboutintel.eu/germany-hacking-reform/

116 For example, the internet exchange point DE-CIX in Frankfurt is one of the largest in the world, with an average overall traffic of more than 6.5 terabits per second at this hub. For more detailed traffic statistics see: https://de-cix.net/en/locations/frankfurt/statistics

117 § 25 BND Act

118 Court of Justice of the European Union. Privacy International v Secretary of State. October 6, 2020, recitals 78-81. https://data.guardint.org/en/entity/35ernv51jnp?page=19

119 Ibid.

- A decision giving an instruction to providers of electronic communication services to carry out general and indiscriminate retention of data (paragraph 139);
- Decisions on national security grounds requiring providers of electronic communication services to retain general and indiscriminate traffic and location data (paragraph 168)
- Decisions authorising automated analysis (paragraph 179);
- The sharing of real time traffic and location data (paragraph 189); and
- National rules which authorise automated analysis (paragraph 192).

Suitability Tests

Serious concerns have been raised in this context about the compatibility of the new BND Act with European case law regarding compelled access through so-called "suitability tests."[120] Those bulk collection suitability tests may be conducted by the BND to assess whether a specific provider or network is suitable for strategic surveillance purposes or to assess the relevance of search terms or create new ones. Suitability tests do not require, as is the case in some other democracies,[121] ex ante authorization involving independent oversight bodies. An order by the president of the BND is only needed to assess the first purpose (suitability of specific telecommunication networks for bulk collection). Moreover, the duration and volume of the data collection in pursuit of suitability tests is not subject to (effective) limitations.[122] While the data collected in the course of suitability tests may generally only be processed for the two purposes, there are important exceptions to this rule when factual indications point to a "significant threat" to individuals or the security of either the Federal Republic of Germany or institutions of either the European Union and its member states, the European Free Trade Association (EFTA) and the North Atlantic Treaty

120 Vieth-Ditlmann, Kilian and Thorsten Wetzling. "Caught in the Act?: An analysis of Germany's new SIGINT reform." 2021. https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform.pdf

121 According to Part 4 Authorisations - Subpart 3 - Practice Warrants - Section 91 - Application for issue of Practice Warrant New Zealand's Intelligence and Security Act 2017 establishes a detailed authorization procedure for testing and training warrants that involves the Chief Commissioner of Intelligence Warrants und des Inspector General. See: https://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM7118938

122 While there is no limitation rewarding the volume of traffic that may be collected by means of so-called suitability tests for either purpose, only the suitability test according to purpose 1 is subject to a six months time limit, which may also be renewed for an unspecified number of times for further six months (§ 24 (2) sentence 2 and 3 BND Act).

Organization (NATO).[123] Force protection of the German military and that of EU, NATO, and EFTA member states also counts as an exception.

Finally, and importantly, the BND may also transmit data from suitability tests automatically (i.e., without further data minimization) to the German Armed Forces[124] where no publicly transparent requirements govern the processing, transfer, and deletion of such data. Moreover, it should be borne in mind that the new judicial and administrative oversight bodies created as part of the 2021 reform of the BND Act have no authority over the use of such data by the German Armed Forces.

The described suitability tests represent a "general and indiscriminate transmission" of personal data to the intelligence service, and are therefore likely not to be "necessary and proportionate" as demanded by the CJEU.

b. Compelled Access in the United States

Law enforcement officials in the United States increasingly seek access to electronic communications, such as emails and social media posts, stored on servers and in data centers. Where law enforcement seeks access to communications, it has a few options, including asking the owner of the device to turn over data voluntarily. More often, law enforcement requests access to data directly from companies. This has led to debate over the extent to which national governments can compel private companies to disclose data, and the degree to which civil liberties and privacy concerns should inform the proper procedure for sharing such data.

In the United States, this debate has largely centered on the Stored Communications Act (SCA), which is part of the broader Electronic Communications Privacy Act (ECPA). Although the SCA generally prohibits certain technology companies from disclosing the contents of electronic communications to third parties, it mandates disclosure to the U.S. government pursuant to a warrant based on probable cause that the communications contain evidence of a crime. As a result, most company privacy policies typically note that they will disclose user data where required by law. However, it may be up to the company to make individual decisions about whether to push back against an overbroad request, or where the legal obligations are unclear.

123 § 24 (7) sentence 1 BND Act

124 § 24 (7) sentence 3 BND Act

Currently, the U.S. government relies upon a handful of different laws and mechanisms to compel access to user information, both domestically and internationally. In general, these legal mechanisms and standards ensure that law enforcement and intelligence agencies do not collect Americans' information unless there is individualized, fact-based suspicion of wrongdoing. The level of suspicion varies depending on the context and the information's sensitivity, but because suspicionless surveillance violates U.S. constitutional principles, "compelled disclosure" in the United States occurs through a variety of legal mechanisms and processes.

The Fourth Amendment of the U.S. Constitution protects against unreasonable searches and seizures, and gave rise to search warrants, which are mostly based on the government demonstrating "probable cause" that a crime has been committed. National Security Letter (NSL) requests are requests for less sensitive information (i.e., no content of communications) that certain government agencies can make when they are conducting national security investigations, under four different federal statutes.[125] Under ECPA, for instance, NSLs compel companies to disclose "the name, address, length of service, and local and long distance toll billing records" of a subscriber to a wire or electronic communications service.[126] As discussed earlier, FISA Section 702 authorizes the U.S. government to target non-Americans located abroad and to collect the content of their communications—notably, the Foreign Intelligence Surveillance Court (FISC) does not review individual applications for particular surveillance targets, but instead approves certifications for certain categories of intelligence information such as counterterrorism.[127] ECPA outlines the standards and processes under which U.S. law enforcement agencies can obtain electronic

125 Currently, NSLs are authorized under four federal statutes: the Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2709), the National Security Act (50 U.S.C. § 3162), the Right to Financial Privacy Act (12 U.S.C. § 3414), and the Fair Credit Reporting Act (15 U.S.C. §§ 1681u, v.). NSLs can only be used to collect information that is considered to be less sensitive (e.g. not the content of communications), and must only meet a lower standard of proof, such as relevance to an authorized investigation.

126 18 U.S.C. § 2709, "Counterintelligence Access to Telephone Toll and Transactional Records" https://www.law.cornell.edu/uscode/text/18/2709

127 The original types of surveillance orders authorized by FISA require the government to show probable cause to believe that the target is a foreign power or an agent of a foreign power. The FISA Amendments Act of 2008 expanded FISA by, among other provisions, adding Section 702 , which authorizes the U.S. government to target non-Americans located abroad and to collect the content of their communications. Under Section 702 the FISC does not review individual applications regarding particular surveillance targets, but instead approves certifications for certain categories of intelligence information such as counterterrorism and approves targeting and minimization procedures.

communications data from tech companies—the most common method for making such requests is through the use of a subpoena.[128]

More recently, the CLOUD Act amended Title II of ECPA to address the question of whether U.S. companies must comply with U.S. law enforcement requests for data access, regardless of where the data is being stored.[129] The CLOUD Act also enables foreign governments who enter into executive agreements with the U.S. government to submit requests for the content of electronic communications directly to U.S. companies, and vice versa—but no bilateral agreements are yet in place.

2. Voluntary Access: Commercial Data Purchases

In addition to compelled disclosure, companies may voluntarily hand over data to law enforcement in a variety of circumstances. Commercial data practices are therefore increasingly intertwined with government intelligence. These voluntary access arrangements may include government entities asking for data from companies on a voluntary basis, government simply receiving offers from companies, or even government entities actively purchasing personal data from private entities. Depending on the type of company involved, there may be no legal restrictions related to voluntary disclosure.

Law enforcement and intelligence services are not blind to the availability of this information stream. In the United States, government entities are increasingly finding ways to obtain this data, which pertains to citizens and non-citizens alike. Over the past few years, the media has surfaced numerous instances of U.S. government agencies circumventing Fourth Amendment requirements, and accountability more generally, by buying data from

128 Under ECPA, there are some cases in which the courts recognize that the requirements of the Fourth Amendment can be met with lower standard than probable cause. As a result, a warrant based on probable cause is not necessary and rather law enforcement, depending on how intrusive the data request is, can obtain a subpoena or a court order, such as a D-order, instead. D-orders require a higher standard than a subpoena. They are most commonly used to obtain non-content, transactional customer records such as the addresses of websites that an individual has visited and the email addresses of other people the individual has corresponded with.Electronic Privacy Information Center, „Electronic Communications Privacy Act (ECPA)“, https://epic.org/privacy/ecpa/

129 This debate was brought up by the Microsoft Corp. v. United States case, as Microsoft refused to turn over data to U.S. law enforcement agencies based on the reasoning that the data was being stored in Ireland.# The passage of the CLOUD Act resolved the dispute between Microsoft and the U.S. government and has now created a more streamlined structure with which U.S. law enforcement agencies can obtain access to data for investigations. Bradford Franklin, Sharon. „The Microsoft-Ireland Case: A Supreme Court Preface to the Congressional Debate“. *Lawfare*. February 22, 2018. https://www.lawfareblog.com/microsoft-ireland-case-supreme-court-preface-congressional-debate

discreet commercial companies known as data brokers.[130] While we are not aware of governments' gaining voluntary access to data outside of purchases, the possibility of voluntary access without any monetary arrangement remains and should also be considered.

The practice of buying data (or gaining other voluntary access to data) means that the government circumvents the need to obtain court orders that would lay out parameters and particularity for the data to be obtained. Accordingly, these private sector practices are not subject to the same judicial oversight, nor are there other oversight mechanisms (congressional or independent) in place to ensure that individuals' civil rights and civil liberties are upheld. When the government buys data (as opposed to accessing it through compelled disclosure mechanisms), there are no retention or minimization requirements or standards, no requirements that the government delete data unrelated to a certain type of investigation, and no transparency requirements—essentially, there are none of the typical democratic controls or privacy safeguards that governments require by law for intelligence collection.

To bring democratic accountability to intelligence practices moving forward, governments must avoid this trend toward purchasing data, and abide by the legal standards for intelligence collection more broadly. That is, they must obtain warrants or otherwise operate within the compelled disclosure mechanisms outlined above, where there are rules in place. Even then, in many cases rules need to be strengthened or more closely followed by the intelligence community. In the U.S. context, where various agencies (and potentially intelligence agencies) are purchasing data for unknown purposes and using the data in unknown ways, Congress must rein them in by passing a clarifying statute and banning the practice of purchasing data from brokers writ large.

a. Background on the Industry

The explosion of data collection by data brokers as well as behavioral profiling for the purposes of online advertising has given rise to a thriving marketplace for personal information, much of which is revealing and intimate. The commercial data broker industry is a rapidly growing multibillion-dollar economy made up of companies large and small that aggregate consumers' information into large datasets by scraping the web or buying data from other companies. This large ecosystem of companies buys, licenses, compiles,

130 Goitein, Elizabeth. "The government can't seize your digital data. Except by buying it." *Washington Post.* April 26, 2021. https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/

analyzes, aggregates, repackages, and sells large sets of personal information—often including very sensitive data such as location information—to anyone willing to pay for it.

A few data brokers have become notorious. ClearviewAI, for example, has been the subject of public scrutiny for scraping publicly accessible photographs, often with names attached, from sites such as Facebook, Instagram, Venmo, and YouTube for facial recognition purposes.[131] The New York Times reported in January of 2020 that over 600 law enforcement offices around the United States had used the service in the preceding year.[132] Additional reports revealed that the FBI, U.S. Department of Homeland Security, and specifically U.S. Immigration and Customs Enforcement (ICE), had also used the company's tool.[133] But far more data brokers operate in the shadows. As far back as 2013, a U.S. Senate report detailed the threats that the data broker industry posed to consumers, finding that they "operate behind a veil of secrecy."[134]

Data brokers repackage people's personal data mostly to cater to advertisers and retail companies, who can then use it to "microtarget" consumers for online advertising—though such data is also valuable to others seeking insights into consumer behavior, such as hedge funds. The information collected and compiled into datasets can include relationship statuses, whether an individual is pregnant, which medicines an individual takes, and which businesses they frequent. Much of this data, especially location data, can be used to predict user movements, especially when combined with social network data and other analytical tools, making it valuable to advertisers and, in turn, brokers. Of all the data that brokers compile and sell, user location data are among the most sensitive and most profitable, leading to the growth of what has been called a new "location data economy."[135] The purchasers of

131 Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It". *New York Times*. January 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

132 Ibid.

133 Ibid.

134 Senate Committee on Commerce, Science and Transportation. "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes". December 18, 2013. https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a

135 Advertising market analysts BIA Advisory Services estimated that location-targeted advertising reached an estimated $21 billion in 2018, according to the New York Times. See: Valentino-DeVries, Jennifer et al.. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret". *New York Times.* December 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

these datasets maintain that their interest is in the patterns that the data reveals about consumers, rather than individual identities.[136] But those with access to the raw data could still use a unique identifier to identify a person without consent. Even without the raw data, one could easily reverse engineer location data by pinpointing a phone that regularly spent time at a certain home address, and using public records to determine who lives there.

b. Current Relevance: The United States, Germany, and the EU

Though these data are ostensibly collected for commerce, recent reporting suggests that, at least in the United States, government law enforcement agencies are rapidly becoming major buyers. There are numerous troubling recent examples involving location data alone. *Motherboard* recently revealed that a data broker named X-mode has been compiling geolocation data from a popular Muslim prayer app (Muslim Pro) and a Muslim dating app (Muslim Mingle), then selling this extremely sensitive data to the U.S. military through defense contractors.[137] Likewise, according to the *Wall Street Journal*, the Department of Homeland Security, ICE, and Customs and Border Protection have been using a commercial database from Venntel Inc. to obtain user location data to detect undocumented immigrants and monitor cell phone activity along the U.S.-Mexico border.[138] This location information—combined with other surveillance tools—has been used to track, arrest, and even deport immigrants across the country.[139] Reports also show that the U.S. Internal Revenue Service also partnered Venntel to identify and monitor suspects in money laundering, cyber, drug, and organized crime cases.[140]

Because investigative reporting surfaced these issues, lawmakers are now delving deeper into understanding the ever-expanding surveillance eco-

136 Newman, Lily Hay. "A Simple Way to Make It Harder for Mobile Ads to Track You". *Wired*. September 21, 2019. https://www.wired.com/story/ad-id-ios-android-tracking/

137 Cox, Joseph. "How the U.S. Military Buys Location Data from Ordinary Apps". *Vice*. November 16, 2020. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

138 Tau, Byron and Michelle Hackmann. "Federal Agencies Use Cellphone Location Data for Immigration Enforcement". *The Wall Street Journal*. February 7, 2020. https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

139 Rivlin-Nadler, Max. "How ICE uses Social Media to Surveil and Arrest Immigrants". *The Intercept.* December 22, 2019. https://theintercept.com/2019/12/22/ice-social-media-surveillance/

140 Lyons, Kim. "Congress investigating how data broker sells smartphone tracking info to law enforcement". *The Verge*. June 25, 2020. https://www.theverge.com/2020/6/25/21303190/congress-data-smartphone-tracking-fbi-security-privacy

system in the United States and beginning to pinpoint the especially problematic role that data brokers play. For example, in 2020, the U.S. House Committee on Oversight and Reform launched an investigation into Venntel's practice of brokering location data to government agencies.[141] In early 2021, the DHS inspector general also announced that, in response to a request from five U.S. senators—Sens. Ron Wyden (D-Ore.), Elizabeth Warren (D-Mass.), Sherrod Brown (D-Ohio), Ed Markey (D-Mass.), and Brian Schatz (D-Hawaii)—his office would be opening an investigation into DHS's purchase of Americans' location data for law-enforcement purposes.[142] Through the investigation, one company that collects and sells consumer data for advertising purposes, Mobilewalla, informed the senators that it had indirectly sold information to DHS to track cell phones without warrants, noting that "selling mobile device data for use by law enforcement agencies is not our business model".[143]

In the EU, the introduction of the GDPR (and the relevant provisions in the European Convention on Human Rights, and Convention 108) have restricted what data data brokers can collect and disclose. Article 5 of the GDPR lays out the general principles according to which personal data must be processed and collected: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

Clear opt-out rights for data subjects and the introduction of a risk-based approach to compliance increase the accountability of data controllers and strengthen the enforcement of data subject rights.[144] Purpose limitation is also a significant safeguard, as it forbids that data is collected and sold for a purpose not defined at the moment of collection.[145] However, it is important

141 House Committee on Oversight and Reform. "Members Launch Bicameral Investigation Into Company Tracking, Collecting, and Selling Consumers' Location Data". June 24, 2020. https://oversight.house.gov/news/press-releases/members-launch-bicameral-investigation-into-company-tracking-collecting-and

142 Tau, Byron. "Homeland Security Watchdog to Probe Department's Use of Phone Location Data". *The Wall Street Journal.* December 2, 2020. https://www.wsj.com/articles/homeland-security-watchdog-to-probe-departments-use-of-phone-location-data-11606910402

143 Tau, Byron. "How Cell Phone Data Collected for Advertising Landed at U.S. Government Agencies," *The Wall Street Journal.* November 18, 2021. https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202

144 Aaron Rieke et al. "Data Brokers in an Open Society". *Open Society Foundation*. 2016, p. 22. https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf

145 Ibid., p. 22.

to note that EU-wide rules and directives are not necessarily applied in full in national laws and actual compliance often falls behind.

In comparison to the United States, these enhanced data subject rights substantially limit the supply of data for intelligence purposes and what products governments are allowed to legally acquire through the private sector. There is nevertheless an active market for personal data, and it is highly likely that intelligence agencies in EU countries make use of these kinds of data sources as well and purchase data on the open market. It is moreover important to note that the private sector is not only relevant in providing data, but also plays a crucial role when it comes to profiling and analysis. This is especially relevant in the context of social media and open source intelligence.

c. Legal Frameworks & Open Questions

Concerningly, the practice of the state purchasing private information from data brokers has been ongoing despite rules from the U.S. Supreme Court that ban the practice. On June 22, 2018, the Court handed down its decision in *Carpenter v. US*, a landmark law enforcement data access case, ruling that under the Fourth Amendment to the U.S. Constitution, law enforcement could not compel a mobile telephone company to turn over the location of a person (for seven days or more) without first obtaining a warrant signed by a judge.[146]

Prior to this ruling, the Stored Communications Act (SCA) allowed compelled production of customer records under a less stringent standard.[147] The Fourth Amendment, which protects against unreasonable searches, was not implicated because the prevailing case law prior to *Carpenter* held that any information given to or collected by a third party lost the amendment's protections. The Supreme Court in *Carpenter* rejected that long-held view and instead decided that, at least when it came to particularly invasive and personal information such as location data held by third parties, individuals should still benefit from Fourth Amendment protections.

146 Carpenter v. United States, 585 U.S.(2018).

147 Section 2703 of the Stored Communications Act allows the government to compel disclosure of transactional records based on "reasonable grounds to believe" that the information is relevant. This standard is less stringent than the Fourth Amendment's "probable cause" warrant requirement. Fernandes, Sean, Supreme Court Addresses Stored Communications Act Cases, American Bar Association, February 15, 2019, https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2018/supreme-court-addresses-stored-communications-act-cases/.

Without access to the SCA's ability to compel records without obtaining a warrant, law enforcement has apparently turned to purchasing those records. As Brennan Center's Elizabeth Goitein pointed out, "[w]hen the government simply incentivizes the disclosure—by writing a large check—the warrant requirement evaporates."[148] *Carpenter* only specifically dealt with the actions of law enforcement, and because it was a narrowly written decision, it does not explicitly address U.S. intelligence agencies. Additionally, the U.S. government has remained silent since the ruling on how, or even whether, it will modify its practices, offering no transparency at all on how the intelligence community interprets *Carpenter*.

Advocates and policymakers have repeatedly pushed for transparency on this very matter—the intelligence community's interpretation of *Carpenter*—with little success. In March 2019, a group of senators wrote to the attorney general inquiring about the government's treatment of metadata in national security cases, and whether it has changed in light of the Supreme Court's decision in *Carpenter*.[149] Sen. Wyden, a member of the Senate Select Committee on Intelligence, sent a list of questions to the Department of Defense in May of 2021 related to the purchase of "internet metadata" and received back answers that were classified—DOD did not reply to Wyden's request to release public answers. Civil society advocates have also called for, at the very least, the government to write and make public a legal memorandum detailing how it interprets *Carpenter* in the context of the Foreign Intelligence Surveillance Act. After some debate, that transparency measure was included in the House-passed version of the USA FREEDOM Reauthorization Act, though it did not become actual law.[150]

In Germany there is no mention of datasets purchased on the private market in the intelligence legislation. The BND Act does not include a provision on the governance and oversight of the service's purchase of data, as the general scope of paragraph 19 of the BND Act is limited to the collection of personal content data (*personenbezogene Inhaltsdaten*) in the context of strategic foreign communications collection. In fact, when it comes to purchased data, only the general mandate description of the BND in paragraph 1 section 2 of the BND Act seems to apply. Those provisions,

148 Goitein, Elizabeth. "The government can't seize your digital data. Except by buying it." *Washington Post.* April 26, 2021. https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/

149 Letter to Attorney General Barr, March 21, 2019. https://www.wyden.senate.gov/imo/media/doc/032119%20Ltr%20to%20DOJ%20Metadata%20post-Carpenter.pdf

150 H.R. 6172, USA FREEDOM Reauthorization Act of 2020, https://www.congress.gov/116/bills/hr6172/BILLS-116hr6172eas.pdf

however, only cover the collection and analysis of information, and we argue that purchases cannot be sufficiently subsumed under this norm in the absence of further, more detailed provisions on the process, safeguards, and oversight. Commercial acquisition of data therefore does not seem to be covered by the comprehensive regulation and oversight regime that the 2021 BND Act reform established.

Not only does the practice of government entities buying citizens' data undermine constitutional requirements and democratic accountability, but the data that the government is buying may not even be accurate. While advertisers' reliance upon such information may merely result in improperly targeted ads and wasted ad dollars, some private sector uses of the data and the government's reliance upon this information can have grave implications. There are many known cases in which individuals were denied housing due to screening companies' incorrect data, often purchased from brokers or pulled from "people search" broker websites,[151] and in which individuals have been rejected from jobs based on background checks with bad data.[152] But, due to the lack of transparency, we do not yet have a complete understanding of how purchased data may be used by our intelligence community, and how serious the implications of bad broker data could be in its hands.

One of the biggest barriers to understanding data brokers' role and impact is the lack of transparency surrounding the industry more broadly—not only for users, but also for regulators. As far back as 2014, the Federal Trade Commission (FTC) called for more transparency around the expansive but largely undiscussed data broker industry. On this front, both Vermont and California have both recently passed laws seeking to shine a spotlight on data brokers, requiring the registration of data brokers operating in those states.[153] Similar legislation has been proposed in the U.S. Congress, at the federal level. However, such registration has had little effect in cutting off the data flows of personal information to and from brokers,

151 Kirchner, Lauren. "When Zombie Data Costs You a Home". *The Markup.* October 6, 2020. https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks

152 Melendez, Steven. "When Background Checks Go Wrong". *Fast Company.* November 17, 2016. https://www.fastcompany.com/3065577/when-background-checks-go-wrong

153 Vermont Statute 9 V.S.A § 2430 requires data brokers to disclose information about their activities to the state, which in turn compiles an online database of registered data brokers. *See* https://sos.vermont.gov/corporations/other-services/data-brokers/. In September 2020, California followed suit by introducing California Civil Code § 1798.99.80, which requires data brokers to register with the state. https://oag.ca.gov/data-brokers

likely due to how data brokers were defined in the bills, and due to the bills' broad exemptions.[154]

B. Roadmap toward Positive Change

In order to avoid potential loopholes and mitigate the risk of future impasses, it is crucial that policymakers consider not only reforms to traditional government surveillance laws, but that they consider private sector data as well—taking both compelled and voluntary access to commercial data into account.

With regard to compelled access to data held by the private sector through lawful means, policymakers should take into account European case law stipulating that such access must be within the limits of what is strictly necessary and proportionate in a democratic society. The CJEU explicitly excludes indiscriminate and general transmission of data from the private sector to the government. Moreover, the CJEU stressed the importance of judicial and administrative oversight when it comes to compelling the private sector to provide access to data.

When it comes to voluntary access to data, the government's purchases of data from the private sector are insufficiently regulated in the legal frameworks both in EU countries and in the United States. This legal loophole is potentially being exploited by intelligence agencies, allowing the government to evade accountability. To avoid this, policymakers in the United States and EU need to take swift action to close legislative loopholes, and in the United States, to enact a comprehensive federal data privacy law.

154 For example, the California law defines data brokers as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202. This definition articulates a distinction between a firm that is a data broker and a firm that engages in data brokerage, based on whether the firm has a direct relationship with the consumers whose data it is collecting and selling. As a result of this distinction, social media companies such as Facebook would not be considered data brokers if they chose to sell their users' information to a third party (known as first-party data mining), as they have a direct business relationship with these users. Additionally, many data-selling and data-sharing firms that play critical roles in the data broker industry would also be exempted from the law. Because of this narrow interpretation of what a data broker is, some experts have characterized the California law as limited in its ability to actually reign in the harms associated with the sale of U.S customer information as a whole. See Sherman, Justin. "Federal Privacy Rules Must Get 'Data Broker' Definitions Right". Lawfare. April 8, 2021. https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right. The Vermont definition is similar to the California definition of data broker, except it also includes firms that license information to a third party. This broader definition of a data broker creates more room to target a range of firms in the data broker industry, and reflects an acknowledgment of the complex data flows that occur between private companies in the country.

1. Closing Legislative Loopholes

U.S. Sen. Wyden has been a leading voice on the issue, calling the government practice of buying Americans' location data a "backdoor to throw the Fourth Amendment in the trash can."[155] For this reason, in early 2021, Sen. Wyden introduced the Fourth Amendment Is Not For Sale Act, which would fill this major gap in statutory law.[156] The Wyden bill would prohibit law enforcement and intelligence agencies from purchasing communications content, geolocation information, and other highly sensitive data which it would otherwise need a warrant to obtain. Significantly, the bill also would limit the government's ability to create new and constitutionally unsound workarounds in the future by establishing that the mechanisms provided in statute (under the Electronic Communications Privacy Act for law enforcement access to Americans' information, and the Foreign Intelligence Surveillance Act for the intelligence agencies) are the exclusive means by which the government may acquire such information about people in the United States.

Ultimately, the Wyden bill would close the loopholes that the intelligence community currently leans on to buy and acquire metadata about Americans' international calls, texts, and emails to family and friends abroad without any FISA Court review. Further, the bill would ensure that when intelligence agencies seek to acquire Americans' location data, web browsing records, and search history, they are required to do so within the framework of the Foreign Intelligence Surveillance Act, and must obtain probable cause orders. (Similar language very nearly passed the Senate in early 2020 via an amendment that Sens. Wyden and Steve Daines (R-Mont.) put forth when Congress considered Patriot Act Section 215 reform legislation.)[157]

155 Patel, Nilay and Adi Robertson. "Donald Trump Trying to Control the FCC is a 'Disaster' Says Sen. Ron Wyden". *The Verge.* August 4, 2020. https://www.theverge.com/2020/8/4/21354244/ron-wyden-fcc-nomination-section-230-trump-order-vergecast-interview

156 Wyden, Ron. "Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act". April 21, 2021. https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-

157 Goitein, Elizabeth. "Surprising Senate Vote Signals New Hope for Surveillance Reform." *Brennan Center.* May 16, 2020. https://www.brennancenter.org/our-work/analysis-opinion/surprising-senate-vote-signals-new-hope-surveillance-reform; Wyden, Ron. "Wyden Opposes Warrantless Government Surveillance of Americans' Internet Browsing History". May 13, 2020. https://www.wyden.senate.gov/news/press-releases/wyden-opposes-warrantless-government-surveillance-of-americans-internet-browsing-history-

The Wyden bill could be even stronger, but is a very important start. The bill as currently drafted only applies to data purchases, once again leaving a small window that the government could exploit—for example, brokers could still provide data to the government on a completely voluntary basis, without any pay. Such arrangements may be of interest to companies seeking to obtain government contracts, or establish rapport with government entities for other reasons, such as avoiding regulation. Nonetheless, in the near term, Congress should take up and pass Wyden's legislation to close this loophole, and ideally strengthen it if there is opportunity.

Even though the market for commercially available data is likely far smaller in Germany than in the United States, commercial acquisition of data needs nevertheless to be included in the intelligence legislation. Clear provisions governing this type of government access to personal data are necessary to make sure that governments do not evade safeguards and accountability mechanisms present for other types of access (i.e., warrants needed in the case of compelled access) by simply purchasing data.

2. Passing Comprehensive Privacy Legislation

In the longer term, a comprehensive data privacy law in the United States could also help—if robust enough. Although the GDPR outlaws sharing data without user consent in the EU, governments may still be able to purchase such data given various exceptions.

In the EU, the GDPR applies to both the public and private sectors and a parallel data protection regulation—the Law Enforcement Directive—applies to "the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data."[158] Therefore, a data broker's obligations would be dictated by the GDPR and a law enforcement agency's obligations would be dictated by the directive.

The GDPR allows data brokers to share personal data with law enforcement if they have a lawful basis under Article 6.[159] The vital interest basis under Article 6(1)(d) could be used if sharing personal data is necessary to protect someone's life. Otherwise, the public task basis under Article 6(1)(e) could

158 Law Enforcement Directive. April 27, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

159 Art 6. General Data Protection Regulation. https://gdpr-info.eu/art-6-gdpr/

be used if the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."[160] Data brokers who compile personal data for marketing or other commercial purposes would need to satisfy the purpose limitation principle because sharing personal data with law enforcement is a new purpose.

However, the GDPR contains a crime and taxation exemption that exempts a law enforcement entity from respecting an individual's data protection rights, including purpose limitation, if compliance would be likely to prejudice the prevention and detection of a crime or the apprehension and prosecution of offenders.[161] Therefore, while EU citizens in the EU have substantially more data protection rights than citizens in the US, EU law enforcement agencies are still able to obtain personal data from data brokers if they can establish a lawful basis for processing.

However, no such comprehensive data privacy law exists in the United States, leaving citizens' data exposed to a range of actors. In the absence of robust federal privacy safeguards, these databases are ready for purchase by predatory actors like loan companies and for-profit colleges,[162] law enforcement agencies, and even malicious foreign actors.

It is long past time for Congress to pass comprehensive privacy legislation. While the EU passed the GDPR in 2016 and it took effect in 2018, the United States lags behind. Currently, U.S. law generally relies on "notice and consent" to protect consumer privacy, but this framework does not give individuals real choices about how their data are used, and it is insufficient to protect user privacy.[163] There is a strong consensus among stakeholders that we need to replace this model with a new approach

160 Ibid.

161 Information Commissioner's Office. "Sharing personal data with law enforcement authorities". https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/#exemption

162 As the 2013 U.S. Senate report noted, "a number of [popular data brokers'] products focus on consumers' financial vulnerability, carrying titles such as 'Rural and Barely Making It,' 'Ethnic Second-City Strugglers,' 'Retiring on Empty: Singles,' 'Tough Start: Young Single Parents,' and 'Credit Crunched: City Families.'" https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a

163 Park, Claire. "How 'Notice and Consent' Fails to Protect Our Privacy." *New America. Open Technology Institute*. March 23, 2020. https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

that places restrictions on how data can be used and gives users enforceable rights over their personal information.[164]

Legislation should codify the eight fair information practices developed by the Organisation for Economic Co-operation and Development (OECD), by including safeguards relating to: the legal bases upon which governments may compel access to personal data; requirements that access meet legitimate aims and be carried out in a necessary and proportionate manner; transparency; approvals for and constraints placed on government access; limitations on handling of personal data acquired, including confidentiality, integrity and availability safeguards; independent oversight; and effective redress.[165]

Finally, comprehensive federal privacy legislation should include all companies that sell data as part of the data brokerage economy. These definitions will therefore be crucial to a federal privacy law's success. As one expert recently pointed out: "Federal privacy legislation will not be sufficiently comprehensive without substantial attention to the data sales and transfers that underpin the data surveillance economy itself. The entity that directly and initially collects a consumer's information is often only the first in a long chain that will acquire it."[166] Accordingly, perhaps additional obligations on data brokers can help address the downstream consequences of how personal data can be used by other parties.

3. Oversight of Data Flows

Finally, comprehensive oversight is needed to follow the flow of data across the private sector (from app developers and platforms to data brokers) and into the public sector (either through compelled access or purchases). These data flows are difficult to follow and have thus far evaded oversight, as few oversight bodies have the broad reach and resources to conduct such a comprehensive review.

164 New America. "Principles for Privacy Legislation". *Open Technology Institute*. November 13, 2018. https://www.newamerica.org/oti/press-releases/principles-privacy-legislation/

165 OECD, Government Access to Personal Data Held by the Private Sector: Statement by the OECD Committee on Digital Economy Policy, December 2020, https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

166 Sherman, Justin. "Federal Privacy Rules Must Get 'Data Broker' Definitions Right". *Lawfare.* April 8, 2021. https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right

The use of commercially available datasets by intelligence services therefore needs to be explicitly included in the intelligence oversight architecture both in Europe and in the U.S. to avoid creative non-compliance. Some countries are already addressing this issue, while many others are far behind. The German legislative framework, for example, does not sufficiently cover such datasets. In the United Kingdom, on the other hand, the oversight body takes the issues of data sets held by the private sector more into account. The Investigatory Powers Commissioner's Office (IPCO) stated that it has conducted "an extensive review of bulk datasets held by third parties to which U.K. intel community had access," so as "to provide assurance that BPD (bulk personal dataset) warrants were being obtained where applicable."[167] The newly created Canadian National Security and Intelligence Review Agency (NSIRA) declared in its annual report that it *"will examine information sharing with private sector organizations,"* and also concretely referred to location data and to the need for warrants even in the case of purchased data.[168]

In the United States, Congress could conduct an investigation into these issues, and/or the PCLOB could play a larger role in overseeing the data flows between the private sector and government. The PCLOB has not, to date, investigated issues pertaining to the government's use of commercial data, outside of its collection practices under FISA Section 702 and Patriot Act Section 215. The PCLOB may be hesitant to take up such matters due to the realities of its resources or its jurisdiction (currently "information sharing practices" of the executive branch are listed as within its jurisdiction, but not necessarily with external parties).[169] Congress could specifically direct the PCLOB to review not just the information sharing practices of the executive branch, but also the sharing practices between the private sector and the government, which have mostly avoided oversight (with the notable exception of the DHS inspector general taking up the issue).

167 Bulk Personal Datasets have been widely criticised by privacy organisations as being too intrusive and allowing for an unprecedented accumulation and analysis of data. Independently of the debate regarding BPDs more specifically, we want to highlight the awareness of the oversight body for the need for warrants in these specific cases.

168 NSIRA. "2019 Annual Report". 2020. Available at: https://nsira-ossnr.ca/wp- content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf, p.46 and p.63.

169 Hatch, Garrett, Privacy and Civil Liberties Oversight Board: New Independent Agency Status, Congressional Research Service, August 27, 2012, https://sgp.fas.org/crs/misc/RL34385.pdf

Chapter 4

Intragovernmental Intelligence Flows

The rapid evolution of surveillance technology is a commonly discussed theme in many policy circles in the United States and across Europe. Less so, are the consequences of the trend whereby the hardware and software for data collection and data processing are increasingly converging across several agencies in the security sector. Whether it is a military intelligence service, police-led intelligence, or customs, border, and migration services, there is a constant and growing demand for different government agencies to cooperate more seamlessly in response to complex, cross-border security threats. This entails data transfers and joint access to common databases and the use of so-called cross-system information analysis platforms, many of which are tailormade by contractors such as Palantir, BAE Systems, Deloitte, IBM, or Rola and others.

The push for more cross-system analysis, as relevant for modern security provision as it may be, should invite lawmakers to ponder more intensely over various associated risks. As indicated by the Council of Europe's Venice Commission, it is not only "the issue of who may query the bulk data collected and for what purposes" but also "lax controls on acquisition, combined with lax minimisation rules and lax controls on access to the data" that is is "a dangerous combination",[170] especially in the context of international security cooperation.

A. Analysis of Common Points of Friction

This section highlights typical risks and unresolved governance aspects regarding the cooperation of various security agencies—both nationally and internationally. It also discusses how they relate to the current transatlantic quest for a better agreement on cross-border data transfers and lawful government access.

170 Venice Commission of the Council of Europe. "Report on the Democratic Oversight of Signals Intelligence Agencies". December 15, 2015. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e

1. Fragmented Legal Frameworks for Similar Data Collection and Data Processing

Unlike other democracies, Germany still sports more than a dozen separate bodies of law on the mandates and democratic governance processes for its intelligence community alone.[171] This stands in stark contrast to countries like the United Kingdom, which has gone to great lengths to establish a main regulatory framework for the use and governance of investigatory powers across several agencies of the security sector (the Investigatory Powers Act). However, German lawmakers continue to focus primarily on the individual security service at hand and have thus far shied away from adopting a more functional approach that focuses instead on the general nature of investigatory powers that the state may use to obtain access to different types of data—irrespective of which agency then deploys them. Their approach to regulation has arguably done very little to improve legal clarity. Quite the contrary, new reforms in 2021 have added to the sheer complexity of the legal framework by inserting various new cross-references to similar yet still different provisions in other laws.

Consider, for example, that the BND's bulk collection practice remains regulated in two separate bodies of laws, namely the BND Act and the Article 10 Act. Depending on whether the bulk data collection pertains to foreign-domestic traffic or foreign-foreign traffic, one must consult the Article 10 Act and the BND Act, respectively. Providers can be compelled to provide government access under two different regulatory frameworks, even though the obligation is very comparable in substance and duration. This causes undue duplications in the authorization and oversight process as well as frustration among the service providers who must unnecessarily navigate different legal regimes.

2. Overlapping and Unsynced Oversight

More generally, it is worth examining whether having different accountability mechanisms and fora for similar investigatory powers defies the protection of human rights, the rule of law, and core democratic principles. This is particularly important in light of growing and more seamless cooperation between different domestic and international security agencies, including the automated sharing of unevaluated personal data.

171 In 2018, the German Parliament published a collection of federal intelligence laws, and this collection consists of 31 separate pieces of legislation.

In Germany, bulk collection is not only regulated in separate laws, it is also overseen very differently—depending on whether it is the foreign intelligence service or the military that practices it. Yet, even with regard to bulk collection by the foreign intelligence service, it is overseen by two separate judicial bodies, namely the G10-Commission and the Independent Control Council.[172] This creates a potential mismatch between the different oversight bodies conducting different types of reviews on similar intelligence collection practices with substantial differences in resources and competencies. Other countries should therefore not follow this model because, amongst other concerns, it carries inherent risks of duplication, turf battles, and likely deficits in the overall accountability and transparency performance.

In the United States, the Title 10-Title 50 debate has long demonstrated the jurisdiction and mismatched oversight problem between military and intelligence activities. This debate is ultimately about the proper roles and missions of U.S. military forces ("Title 10") and intelligence agencies ("Title 50").[173] One crux of the debate has been the vast differences in oversight between military operations and intelligence activities. Former CIA General Counsel Jeffrey H. Smith summarized the issue, noting "if the activity is defined as a military activity ('Title 10') there is no requirement to notify Congress, while intelligence community activities ('Title 50') require presidential findings and notice to Congress." The natural inclination for executive branch lawyers, according to Smith, is to prefer the Title 10 paradigm to escape congressional notification requirements.[174]

Bulk data collection through signals intelligence and computer network exploitation (hacking) are practices that both the German armed forces and Germany's foreign intelligence service (BND) regularly use.[175] Computer network exploitation is particularly noteworthy in this regard: It is „the Swiss army knife of surveillance" because it combines many powerful surveillance functions in one powerful tool. This can include audio, visual, email, texts,

172 See, the remit of these bodies in §15 of the Article 10 Act and § 41 of the BND Act, respectively.

173 Andru E. Wall. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Activities, Intelligence Operations, & Covert Action". Harvard National Security Journal, Vol. 3. 2011. https://www.soc.mil/528th/PDFs/Title10Title50.pdf

174 Ibid.

175 See also Vieth-Ditlmann, Kilian and Thorsten Wetzling. "Caught in the Act?: An analysis of Germany's new SIGINT reform." 2021. https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform.pdf

communications metadata, online activity surveillance as well as location tracking through one single method.[176]

While these practices by the civilian intelligence services and military intelligence are often closely aligned, often for a good reason, such as force protection, they remain subject to substantially different oversight bodies with radically different control densities.[177] The requirements for data processing, transfers, and deletion within the armed forces are fewer and less transparent. There is, however, a need for a more holistic perspective, for example, when the BND automatically transmits data that it collected as part of its "cold-start collection via suitability testing" (which does not carry data minimization requirements) to the German armed forces (§ 24 (7) sentence 3 BND Act). Comparing the oversight remits and resources for civilian intelligence with that for military intelligence and recalling the increased cooperation between these actors, it is deplorable that the newly created German judicial and administrative oversight body (ICC) will have no mandate to review the use of such data by the German armed forces. This is done very differently, for example, in Canada. See the discussion further below.

Furthermore, the practice to establish limited oversight mandates for separate oversight bodies runs counter to the norm established in international conventions, notably the modernized Convention of the Council of Europe for the protection of individuals with regard to the processing of personal data.[178] As observed recently by the Dutch intelligence oversight bodies CTIVD and TIB in their memo on that convention, "when appointing the oversight body/supervisory authority (i.e., Article 11.3, 15, and 16(2) of the Convention), it must be clear that the entire national security domain falls under the responsibility of the oversight body or bodies to be appointed."[179]

176 Smith, Stephen W. "Clouds on the Horizon: Cross-Border Surveillance under the US Cloud Act." 2021, p. 129. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3917893

177 See Wetzling, Thorsten. "Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts". February 21, 2021, p.16f. https://www.bundestag.de/resource/blob/823556/760abb7961fa7df144e1bc834702d44f/A-Drs-19-4-731-F-data.pdf

178 Council of Europe. "Convention 108+ - Convention for the protection of individuals with regard to the processing of personal data". 2018. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

179 CTIVD and TIB. "Memo CTIVD and TIB on Convention 108+". February 17, 2021. https://english.ctivd.nl/documents/publications/2021/02/17/memo-en. For a more detailed discussion on the relevance of Article 11 of this modernised Convention for democratic intelligence in Europe, see: Wetzling, Thorsten and Charlotte Dietrich. "Report on the need for a guidance note on Article 11 of the modernised Convention". June 11, 2021. https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512

U.S. government "fusion centers" have also brought this information-sharing issue into focus. Fusion centers are state-owned and operated centers, funded by the Department of Homeland Security, that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between state, local, tribal and territorial; federal; and private sector partners.[180] According to the Brennan Center, which has done in-depth analyses of fusion centers: "the theory is that in their normal activities, state and local police come across information that might be useful in uncovering terrorist plots. The Department of Homeland Security funded and promoted fusion centers as a means to harvest this information and provide it to intelligence analysts so they could 'connect the dots' and prevent terrorist attacks... But as early as 2007, leaked reports from fusion centers showed serious problems with their intelligence gathering. Instead of looking for terrorist threats, fusion centers were monitoring lawful political and religious activity."[181]

Most recently, the January 6, 2021 insurrection in the United States has brought attention back to these issues, as intelligence sharing between the various domestic U.S. agencies has come to the forefront—some officials blaming failures in intelligence sharing for the severity of the attack.[182]

B. Roadmap toward Positive Change

As government agencies are increasing their interconnectedness thanks to the rapid evolution of surveillance hardware and software, there is also a substantial increase in automated data transfers and cross-system information analysis between different actors of the security sector. In light of this, narrow horizontal oversight mandates and fragmented legal frameworks can unduly contribute to obfuscation and an increase of accountability gaps and transparency deficits. This also carries the risk of creative non-compliance or malfeasance. Therefore, U.S. and EU policymakers should be interested in learning how to overcome such risks, especially in view of a potential review of a new cross-border data sharing agreement. A future European Court of Justice or a

180 Department of Homeland Security. "Fusion Centers". September 19, 2019. https://www.dhs.gov/fusion-centers

181 Patel, Faiza and Michael Price. "Fusion Centers Need More Rules, Oversight". *Brennan Center for Justice*. October 18, 2012. https://www.brennancenter.org/our-work/research-reports/fusion-centers-need-more-rules-oversight

182 Alfaro, Mariana. "U.S. Capitol Police's failure to share intelligence internally crippled its response to Jan. 6 attack, former official says". *Washington Post.* October 11, 2021. https://www.washingtonpost.com/politics/jan-6-attack-capitol-police-whistleblower-congress/2021/10/11/18c38502-2aa2-11ec-985d-3150f7e106b2_story.html

U.S. court will have to assess whether robust safeguards exist in both entities to legitimize lawful government access to personal data obtained in such contexts, many of which also concern data held by the private sector.

1. Establishing Holistic All-Inclusive Oversight Remits

Fortunately, as argued below, there are positive examples from which to draw inspiration for a rights-based cross-border data agreement. While the German government sees no problem with the above-mentioned mismatch of having different oversight bodies review similar intelligence collection practices with substantially different resources and review competencies,[183] recent statutory reforms in Canada[184] and the United Kingdom[185] point in a notably different direction.

The new Canadian oversight body, NSIRA, for example, can "review any activity in the federal government that relates to national security or intelligence". The organization calls it "horizontal, in-depth interagency review.".[186] It [...] allows NSIRA to break down the previously compartmentalized approach to review and accountability, and replace it with horizontal, in-depth interagency review."[187]

While compartmentalized oversight setups might lack the general overview over all data processing and data transfers across national security agencies, they have become specialized, which is also an important feature. Hence, lawmakers should be cautious not to merely opt for centralized oversight at the expense of resources and precision in investigations.

183 Federal Government. "Answer of the Federal Government to the minor interpellation 19/2583". January 26, 2021, p.5. https://dserver.bundestag.de/btd/19/261/1926120.pdf

184 Bill C-59 entered into force on 21 June 2019. The new Canadian oversight body NSIRA can access "classified information in the possession or under the control of *any* department or agency (except Cabinet confidences)". In: NSIRA. "2019 Annual Report". 2020, p. 16. https://nsira-ossnr.ca/wp- content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf (emphasis added).

185 In the 2016 Investigatory Powers Act (IPA), the Investigatory Powers Commissioner's competencies are defined by whether or not investigatory powers are exercised no matter which government agency is involved: "the Investigatory Powers Commissioner must keep under review ... the exercise by public authorities of statutory functions" (IPA, section 229 (1), emphasis added). It is thus not restricted to reviewing certain intelligence agencies only. Exceptions to these provisions are defined in IPA 229 (4).

186 NSIRA. "2019 Annual Report". 2020, p. 20. https://nsira-ossnr.ca/wp- content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf

187 Ibid., p.16

2. Multilateral and Transatlantic Oversight Cooperation

Transnational threats prompt closer cross-border cooperation among intelligence services, but increasingly also involve a range of other security agencies including the military, police, and other branches of the security sector. Typically, joint databases are run multilaterally, with all participating services adding and accessing data, albeit with several restrictions and caveats. In such cases, there is a need for creating joint responsibility among the participating states for the database and subsequent data processing.

The Dutch Intelligence Oversight Body's (CTIVD) 2018 report on the European Counter Terrorism Group's (CTG) operational database in the Netherlands provides a useful illustration of typical open questions related to government responsibility and oversight in the context of international intelligence cooperation. The CTG facilitates, amongst other things, the multilateral exchange of evaluated data on individuals who have traveled to and returned from conflict areas. The CTIVD concluded, for example, that safeguards for the protection of fundamental rights were not sufficiently addressed and recommended setting up multilateral controls.[188]

While some states may accept responsibility and oversight for their services' submissions to joint databases, the subsequent data processing is rarely covered, certainly not if the database is not hosted by a foreign government on a foreign territory. This creates the potential for severe accountability gaps: Who is held responsible for the processing of erroneous data? Furthermore, as acknowledged by the Dutch government, there is a pressing need

188 CTIVD. "Review report 56 on the exchange of personal data on (alleged) jihadists by the AIVD". April 26, 2018. https://english.ctivd.nl/investigations/r/review-report-56-onthe-exchange-of-personal-data-on-alleged-jihadists-by-the-aivd

to ensure effective oversight over the use of joint databases, possibly in the form of multilateral oversight.[189]

The forward-looking recommendations by the Dutch oversight body with respect to multilateral oversight is something that policymakers should pay greater attention to— beyond the complex accountability deficits of the European CTG's operational platform - to which the United States has apparently an observer status.[190]

C. Summary

EU member states and the United States may find it increasingly difficult to defend the fact that data processing across their respective security sectors is done with similar investigatory powers, yet is governed and overseen by substantially different statutes, review bodies, mandates, and with different resources.

According to a recent study by the Geneva Centre for Security Sector Governance – DCAF and NATO's Parliamentary Assembly, "a sub-standard legal base, insufficient expertise and little public attention have deprived military intelligence oversight of effectiveness in too many countries and for too long. In most parliaments there is no routine oversight over military intelligence."[191]

189 "Bearing joint responsibility also requires joint, multilateral oversight. After all, the different national oversight bodies will each face the question whether the service they are overseeing gives sufficient implementation to the joint responsibility that the service bears. National oversight alone is insufficient in this case. The government recently agreed that there must be multilateral oversight. [...] it is necessary that the safeguard of independent, adequate and effective joint oversight is included in a common data protection framework for the CTG database.
[...] Another option would be to explicitly divide the oversight tasks, with one or a few oversight bodies being charged with organising the joint oversight. [...] One or more oversight bodies could be assigned the responsibility to perform the oversight on behalf of all of them. [...] A third option would be to institute overarching, international oversight. To that end a new international oversight body would have to be created, to which certain oversight powers are assigned. This is the most far-reaching option and would require a public-law basis, such as a treaty between States." CTIVD. "Review report 56 on the exchange of personal data on (alleged) jihadists by the AIVD". April 26, 2018. https://english.ctivd.nl/investigations/r/review-report-56-onthe-exchange-of-personal-data-on-alleged-jihadists-by-the-aivd

190 Jirat, Jan and Lorenz Naegeli. "The Club de Berne: a black box of growing intelligence cooperation". *about:intel*. April 1, 2020. https://aboutintel.eu/the-club-de-berne/

191 Jasutis, Grazvydas et al.,"Parliamentary Oversight of Military Intelligence". *DCAF*. 2020, p. 39. https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf

Bulk collection by military intelligence services can present the same risks to fundamental rights as similar practices by (civilian) intelligence agencies. Yet, oversight over military intelligence's access and use of such data is rarely as comprehensive and resourceful as intelligence oversight has become in some jurisdictions.

Given the privileged partnership between the military and the civilian intelligence services, a comprehensive legal framework would go a long way to mitigate the inherent risk of creative non-compliance. For example, a government may be inclined to maintain separate oversight regimes and accept accountability deficits as part of a hidden motive to foster "autonomy-enhancing capacities and opportunities to somehow forestall, neutralize, transform, resist, or overcome the societal constraints imposed upon them."[192] To illustrate this further, the federal German government may be inclined to delegate more tasks to intelligence units of the military due to the fact that processing of data from bulk collection there is far less rigidly overseen there than for the BND's data processing. This is unlikely to be the sole decisive criteria for such data transfer decisions, but good legislative and oversight practice ought to be more mindful of such potentially hidden *raisons d'état*, too.[193]

Accordingly, a more comprehensive framework with reduced but strengthened oversight bodies would limit the risks to oversight effectiveness discussed above.

192 Nordlinger, Eric A. "On the Autonomy of the Democratic State". 1982, p. 30.

193 Koenig-Archibugi, Mathias. "International Governance as New Raison d'Etat? The case of EU Common Foreign and Security Policy." *European Journal of International Relations*. 2004. https://journals.sagepub.com/doi/10.1177/1354066104042933

Chapter 5

Discussion and Recommendations

From overbroad government collection, insufficient purpose limitations, and vague data processing requirements, to ill-equipped oversight and redress mechanisms, and easy access from the private sector and other parts of government, our data is often at risk even in democratic nations with oft-debated intelligence laws and practices. Many open or unresolved challenges in the governance of intelligence collection have led to accountability deficits that betray citizens' trust, as well as other nations' trust—democracies across the world are grappling with similar challenges on this front. More can and should be done to square national practice with common international principles of democracy, rule of law, and human rights that mature democracies proudly share. While the CJEU's *Schrems II* decision highlighted how the current laws inadequately protect the right of non-nationals to judicial redress in the United States, further surveillance and intelligence reform is urgently needed in both the EU and the United States.

Our respective democracies took centuries to establish their unique brand of rule, and our legislatures and legal systems operate quite differently from country to country. This makes it difficult to build a successor to the Privacy Shield because it needs to contain adequate protections and regard for fundamental rights in a way that respects national sovereignty and allows parliaments to legislate according to their established norms. A one-size-fits-all global gold standard for intelligence and surveillance governance is therefore not realistic.

At the same time, we also caution strongly against adopting standards in international cross-border data agreements that merely amount to the lowest common denominator. Some U.S. experts have questioned the need for the United States to take drastic action in response to *Schrems II*, arguing that surveillance practices in some EU member states are comparable to those in the United States, and therefore similarly do not live up to the CJEU's standards. Accordingly, legal expert Peter Swire suggested that it is "unrealistic for the EU to demand changes to U.S. national security legislation

when European countries themselves are not averse to similar practices."[194] Further, some argue that U.S. oversight mechanisms are more robust than what exists in many EU member states. However, one of the main entities these critics point to is the PCLOB, which has recently struggled to conduct effective oversight likely due to lack of capacity, resources, and vacancies.[195] Rather than debating whose practices are worse, democracies should race to the top when it comes to protecting civil liberties and other fundamental rights, adopting stronger safeguards and oversight mechanisms that can serve as models.[196]

While we do not yet know the outcome from recent negotiations surrounding the Privacy Shield follow-up agreement, we are hopeful that the new agreement will go beyond a quick fix, and address some of the major questions regarding proportionate government access to personal data. But generally, closed door conversations between the U.S. government and the EU Commission do not provide the robust dialogue needed to achieve a balanced and comprehensive result that will protect civil liberties and satisfy all the relevant courts for years to come. Instead, we need a more inclusive dialogue that brings together government and oversight body representatives with academics, civil society, and the private sector. This will inevitably broaden the scope of these conversations to consider topics such as government purchases of data and other modes of government access to personal data.

Of course, there are strong economic pressures to find a quick resolution for the cross-border data impasse. Restricting data flows can sharply reduce trade volume, reduce productivity, and drive up prices for industries that increasingly rely on data.[197] As the data flows between the United States and EU

194 Mark Scott, POLITICO Digital Bridge: Privacy Shield is Stuck - COVID Changed Everything -- What Next on Digital Tax?, POLITICO, July 15, 2021, https://www.politico.eu/newsletter/digital-bridge/politico-digital-bridge-privacy-shield-is-stuck-covid-changed-everything-what-next-on-digital-tax/

195 Matthew Guarglia and Cindy Cohn, PCLOB "Book Report" Fails to Investigate or Tell the Public the Truth About Domestic Mass Surveillance, Electronic Frontier Foundation, June 30, 2021, https://www.eff.org/deeplinks/2021/06/pclob-book-report-fails-investigate-or-tell-public-truth-about-domestic-mass; Civil Society Letter to President Biden Regarding PCLOB Vacancies, September 7, 2021, https://cdt.org/wp-content/uploads/2021/09/2021-09-07-PCLOB-Vacancies-Coalition-Letter.pdf

196 For a recent compendium of good legal standards and oversight practice on the many governance challenges tied to bulk collection of personal data by intelligence services, see: https://www.intelligence-oversight.org/

197 Cory, Nigel and Dascoli, Luke, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How To Address Them, Information Technology & Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

continue to remain in question, large companies may consider storing personal data locally within the EU (data localization), as it may be an easier alternative to dealing with messy and unclear legal questions. However, not only does this data localization present risks to the economy and internet freedom, but it also may not resolve the concerns outlined in *Schrems II*. First, an alternative solution such as data localization may not be affordable or realistic for many small and medium-sized companies that rely on cross-border data transfers. Additionally, data localization in the EU might not fully address concerns regarding government access, as the data may still be accessible to the company in other countries where it operates.

It remains very unclear whether U.S. administrative actions would satisfy the CJEU, therefore legislative action will likely be necessary to limit U.S. intelligence community access to EU citizens' personal data at the outset, and especially to create a right for EU citizens to seek redress in U.S. courts. However, because legislation moving through the U.S. Congress is rather unlikely in the near-term, administrative action may suffice in the short-term and show good faith on the U.S. government's part while attempts at more permanent legislative change are underway.

As they draft new legislation, our democracies can write exceptions to the standard procedures into their legal frameworks that are more clearly defined, allowing governments to respond to imminent dangers. By and large, much more can be done to reconcile the valid needs of security agencies (to access personal data in the pursuit of their important mandate) with the protection of privacy and other rights and freedoms.

As these transatlantic dialogues continue, some analysts have suggested another alternative would be for the United States and EU to abandon the idea of a quick Privacy Shield replacement and instead begin negotiations for a broader digital trade agreement.[198] Such an agreement could consider cross-border data flows alongside other issues, such as how to handle customs duties on electronic transmissions, ensuring online consumer protection, legal frameworks for data subject rights, prohibiting forced technology transfer, promoting open government data, cybersecurity cooperation, etc.[199] This could prove difficult, however, as the EU has been reluctant to

198 Congressional Research Service, U.S.-EU Privacy Shield and Transatlantic Data Flows, September 22, 2021, https://crsreports.congress.gov/product/pdf/R/R46917

199 "As a possible template, negotiators could look to the U.S.-Japan Digital Trade Agreement, concluded in October 2019. The USTR has called it the "most comprehensive and high-standard trade agreement" negotiated on digital trade barriers and said it could set precedents for other talks." https://crsreports.congress.gov/product/pdf/R/R46917

include requirements to ensure cross-border data flows or prohibit localization in its trade agreements, maintaining that data protection is a fundamental right and therefore not negotiable within trade agreements—the EU prefers using adequacy decisions instead.[200] The ongoing legal uncertainties surrounding the CLOUD Act and cross-border law enforcement access to data also need to be addressed, thus, it may make sense to consider these very related issues alongside the surveillance questions raised by *Schrems II*.[201]

Regardless of whether the U.S. and EU governments take up such a comprehensive approach in the current moment, they must immediately address intelligence collection practices, government access to private sector data, and flows of data through other areas of government into the intelligence community.

Throughout Chapter Two we discussed how opaque legal frameworks for surveillance and intelligence, and oversight mechanisms that aren't fit-for-purpose, are incommensurable with the rule of law and core principles of democratic governance. They are often also a hindrance for individuals trying to understand and enforce their rights in the EU and United States. Recently, the European Court of Justice and the European Court of Human Rights, as well as the German Constitutional Court, reprimanded lawmakers for adopting overly permissive legal frameworks on data collection and retention. Lawmakers on both sides of the Atlantic should seize the opportunity to write robust safeguards into their laws, and enact provisions that deter and sanction disproportionate government access to personal data when it comes to

200 European Union, Agreement Between the European Union and Japan for an Economic Partnership , Chapter 8, Trade in Services, Investment Liberalization, and Electronic Commerce, Article 8.3, entered into force February 1, 2019, https://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement/; CRS In Focus IF11120, U.S.-Japan Trade Agreement Negotiations, by Cathleen D. Cimino-Isaacs and Brock R. Williams

201 For instance, as one legal expert has pointed out, U.S. jurisprudence is currently unsettled as courts work to apply the law to new surveillance techniques such as smartphone tracking and computer hacking, so foreign governments may rightfully be hesitant to enter into a CLOUD Act agreements permitting the U.S. to engage in such activities on their soil. Relatedly, "several EU countries have already recognized the special dangers posed by government hacking--to privacy, internet security, and foreign relations--and have developed a panoply of protections to mitigate those risks. By contrast, the U.S. has failed to enact any special substantive and procedural protections against the risks posed by such intrusive surveillance." Smith, Stephen W., Clouds on the Horizon: Cross-Border Surveillance Under the US CLOUD Act (March 10, 2021). Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, chapter 8 (edited by Federico Fabbrini, Edoardo Celeste, John Quinn) (2021), Available at SSRN: https://ssrn.com/abstract=3917893. In both CLOUD Act agreement negotiations and negotiations surrounding the Schrems II decision, these surveillance methods and the outstanding legal questions surrounding them should come into play and must be addressed.

various intelligence collection practices. More concretely, EU and U.S. lawmakers should:

- Enable standing in court that is not hindered by secrecy regulation, where possible (e.g., make it independent from notice), and professionalize the national complaint mechanisms for citizens and non-nationals.
- Establish a clear and consolidated legal framework for investigatory powers across the intelligence and security sector.
- Regulate all types of bulk data access transparently, such as commercial data purchases, suitability tests, and interception of machine-to-machine communications;
- Apply the same standards and safeguards that pertain to personal content data to the collection and processing of metadata.
- Enact effective purpose limitations for data collection to limit uncontrolled data transfers and re-use of data outside or within governments.
- Establish a consolidated judicial authorization mechanism for all foreign intelligence collection warrants in order to eliminate duplications and inefficiencies.
- Expand the independent approval powers of oversight bodies to cover bulk data analysis (examination warrants), suitability tests (testing and training warrants), and commercial data buying (data acquisition warrants).
- Provide oversight bodies with sufficient resources and expertise to perform end-to-end oversight: This requires adjustments to the oversight remits as well as capacity building and training to help ensure that the entire process of surveillance is subject to robust and data-driven oversight;
- Establish higher standards for effective review, notably by establishing and improving an adversarial process within the authorization process to defend the interests of certain groups affected by surveillance (i.e.,non-nationals and certain protected professional groups), and by endowing oversight bodies with binding enforcement powers, including the power to prohibit certain data collection and to require data destruction. In addition, oversight bodies should possess genuine sanctioning powers in the context of foreign intelligence collection.
- Codify comprehensive public reporting obligations for the oversight body.

In Chapter Three of the report, we confronted a somewhat novel issue for the EU and the United States: how governments circumvent current legal standards to access commercially available data, namely through purchases of data from the private sector. This particular type of "voluntary access," which exploits legal loopholes, appears to be on the rise in the United States, where numerous reports over the past two years have

exposed government agencies buying data on citizens and non-citizens from data brokers, especially location data.

To better safeguard individual rights when it comes to government access to commercial data, governments and parliaments should:

- Consider and enact legislation both in the United States and Europe that would close these loopholes, such as Sen. Wyden's Fourth Amendment is Not for Sale Act—governments should not be able to evade accountability mechanisms by purchasing data.
- Pass comprehensive privacy legislation in the United States that codifies the seven principles developed by the OECD. While the EU is considerably better positioned in this regard thanks to the GDPR, it should continue to work on a coherent enforcement of the GDPR.
- Ensure more comprehensive oversight within existing bodies—and provide those bodies the resources required to conduct such oversight—or via new oversight bodies where necessary.

In Chapter Four of this report, we examined different modes of cooperation between military and civilian intelligence, and discussed risks associated with automated data transfers, joint databases, and the use of common software such as cross-system information analysis platforms. Lawmakers interested in addressing and reducing obfuscation, accountability gaps, and transparency deficits tied to the automated cooperation of different actors of the security sector should:

- Adjust and consolidate their legal frameworks for the governments' use of investigatory powers to avoid duplication and important government practice falling through the cracks. Lawmakers are advised to adopt a functional approach to the regulation of investigatory powers that focuses on the general nature of investigatory powers rather than the agency that deploys them.
- Avoid having entirely different accountability mechanisms for reviewing the use of similar investigatory powers by different actors of the security sectors who are also in intense cooperation with one another. Instead, European and U.S. lawmakers should follow the examples of the United Kingdom

and Canada, and ensure "that the entire national security domain falls under the responsibility of the oversight body or bodies to be appointed."[202]

Ultimately, through *Schrems II*, the CJEU has forced the U.S. government to reconsider its surveillance laws and practices in order to ensure future transatlantic data flows. But, as demonstrated throughout the report, *both* the United States and EU member states should rethink and redesign their surveillance standards and safeguards more holistically. There is ample room for progress on both sides of the Atlantic to ensure privacy rights are preserved regardless of one's nationality, location, or where their data is transferred. The United States and EU member states must also do much more to render their oversight and redress mechanisms fit for purpose.

202 CTIVD and TIB. "Memo CTIVD and TIB on Convention 108+". February 17, 2021. https://english.ctivd.nl/documents/publications/2021/02/17/memo-en. For a more detailed discussion on the relevance of Article 11 of this modernised Convention for democratic intelligence in Europe, see: Wetzling, Thorsten and Charlotte Dietrich. "Report on the need for a guidance note on Article 11 of the modernised Convention". June 11, 2021. https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent, non-profit think tank working at the intersection of technology and society. SNV's core method is collaborative policy development, involving experts from government, tech companies, civil society and academia to test and develop analyses with the aim of generating ideas on how governments can positively shape the technological transformation. To guarantee the independence of its work, the organization has adopted a concept of mixed funding sources that include foundations, public funds and corporate donations.

About the authors

Dr. Thorsten Wetzling heads the SNV's research unit on basic rights, surveillance and democracy. He currently directs the European Intelligence Oversight Network (EION), a collaborative research project to support and challenge intelligence oversight bodies across Europe. He is also a Principal Investigator for the international research consortium GUARD//INT which aims to build empirical and conceptual tools to better understand the limits and potential of intelligence oversight mechanisms. Thorsten is also founder and editor-in-chief of aboutintel.eu – a European discussion forum on surveillance, technology and democracy.

Dr. Thorsten Wetzling
twetzling@stiftung-nv.de

Charlotte Dietrich is a project manager for Digital Rights, Surveillance and Democracy at SNV where she works on strengthening democratic oversight of intelligence services and connecting oversight agencies from all over Europe through the European Intelligence Oversight Network (EION). She also manages the intelligence-oversight.org plattform, an interactive database on international good practices in SIGINT governance. Charlotte holds a Master's degree in National Security Studies from King's College London's Department of War Studies and studied Political Sciences at Sciences Po Paris and the Saint Petersburg State University for her undergraduate studies.

Charlotte Dietrich
cdietrich@stiftung-nv.de

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. OTI promotes universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

About the author

Lauren Sarkesian is senior policy counsel at New America's Open Technology Institute, focusing on electronic surveillance and tech privacy issues.

Before joining OTI, Sarkesian served for over six years in legislative roles within the White House, U.S. Senate, and U.S. House of Representatives. Most recently, Sarkesian was counsel to Rep. Don Beyer (D-Va.), where she focused on science and technology, judiciary, and government oversight issues. Her work there included drafting legislation pertaining to government use of facial recognition technology. Previously, Sarkesian served in the White House Office of Legislative Affairs, where she worked to advance President Obama's nominees and legislative priorities in the Senate, especially criminal justice reform legislation. Sarkesian also served as a law clerk to the Senate Health, Education, Labor, and Pensions Committee oversight team under Chairman Sen. Tom Harkin (D-Iowa), contributing to investigations related to civil rights violations in our education systems.

Sarkesian is from the Detroit area and graduated from the University of Michigan (B.A.) and Loyola University Chicago School of Law (J.D.).

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:
Alina Siebert