NEW AMERICA

April 2021

Strengthening Surveillance Safeguards After *Schrems II*

A Roadmap for Reform

Sharon Bradford Franklin, Lauren Sarkesian, Ross Schulman, & Spandana Singh

About the Author(s)

Sharon Bradford Franklin is policy director for New America's Open Technology Institute. Prior to joining OTI, Franklin served as executive director of the Privacy and Civil Liberties Oversight Board.

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

Ross Schulman is a senior counsel and senior policy technologist at New America's Open Technology Institute.

Spandana Singh is a policy analyst with New America's Open Technology Institute.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

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. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Executive Summary

In the July 2020 *Schrems II* case, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield. Over 5,300 companies relied on the Privacy Shield to facilitate transatlantic data transfers between the United States and Europe for services including social media, messaging, cloud services, and email. The CJEU found that 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 the personal data of European Union (EU) citizens, and that the United States lacks any mechanism to provide effective redress for EU citizens whose data is transferred to the United States. The decision has created ambiguity around the future of trade between businesses in the United States and the EU.

This report puts forth recommendations for measures that the U.S. government can implement without the need for congressional action. We do not suggest that every measure we recommend is strictly required by the *Schrems II* decision, nor can we forecast that if all of the recommendations we set forth here are adopted, this would fully satisfy the CJEU. Rather, we seek to outline a package of reforms that address the *Schrems II* decision, that increase privacy safeguards for both U.S. persons and non-U.S. persons, and that should be achievable in the near term.

Reforms to Collection and Targeting

Reforms that would address collection and targeting practices under Section 702 and EO 12333 would limit the risk of intrusion on the privacy rights of both U.S. and non-U.S. persons, and would likely be the most effective means of protecting those rights. The U.S. government should:

- Build upon Presidential Policy Directive 28 (PPD-28) by applying the six-category *use* limits for bulk data in PPD-28 to restrict the permitted purposes for **bulk *collection***.

- Adopt binding rules to ensure that **bulk collection** is only conducted when it meets the principles of **necessity and proportionality** under international human rights law.

- Commit in its Section 702 targeting procedures to following the **definition of foreign intelligence information under FISA** that applies to U.S. persons, namely that information must be "necessary to" the United States' ability to protect against threats, rather than the

broader "relates to" standard that applies for foreign intelligence information regarding non-U.S. persons.

- Strengthen and narrow the **standard for targeting under Section 702** from the current standard, which only requires that the targeting will be "reasonably likely to return" foreign intelligence information related to one of the 702 certifications.

- Commit through an executive order or directive that it will **not reinstate "about" collection** under Section 702, ensuring that the National Security Agency only collects communications that are "to" or "from" a target.

- Remove the term "foreign persons" from the **definition of foreign intelligence under EO 12333** to ensure that collection is limited to information regarding foreign governments, organizations, and terrorists rather than any foreign individual.

- Strengthen the **standard for surveillance targeting under EO 12333** by, at a minimum, incorporating the Section 702 targeting standard of "reasonably likely to lead" to foreign intelligence.

- Require the government to seek and create procedures for **FISA Court post hoc review of targeting decisions under Section 702, as part of the annual recertification of the program**. These new procedures should be incorporated into the Section 702 targeting procedures.

Minimization Reforms

Minimization is the broad term that covers how the intelligence agencies may access, use, retain, and share collected data. The U.S. government should:

- Adopt more **robust and transparent limits** on how collected information regarding specific individuals—regardless of nationality—**may be used**.

- **Raise the bar for queries** seeking information about residents of other countries by extending the documentation requirement (for a statement of facts supporting the query term) to cover all queries seeking information about any specific person—regardless of that person's nationality or location—under both Section 702 and EO 12333.

- **Lower the default time period for retention** of data under both Section 702 and EO 12333 to three years, and examine and narrow the

exceptions to default retention rules, such as the exception for encrypted communications.

- Require that when intelligence agency personnel actually review collected information and do not affirmatively assess it to qualify as foreign intelligence information, they **must purge that data** rather than waiting until expiration of the default retention period.

Improving Transparency

Greater transparency for the rules governing U.S. surveillance is needed and will benefit U.S. and non-U.S. persons alike. The U.S. government should:

- **Disclose the categories** that are the subjects of the **Section 702 certifications** approved by the FISA Court, thereby outlining the scope of permitted 702 surveillance.

Creating Meaningful Redress

Targets of U.S. surveillance under Section 702 and EO 12333, including EU citizens, lack a mechanism through which they can seek redress in U.S. courts. The CJEU in *Schrems II* emphasized that effective judicial redress requires that individuals are entitled to hearings before an independent and impartial tribunal. The U.S. government should:

- Provide a **mechanism for independent judicial redress or standing** to bring challenges to surveillance practices in U.S. courts. Proposals for administrative solutions may be worth considering and could be a helpful first step to show good faith in negotiations. But in order to fully meet the redress standard set forth by the CJEU, legislation will be needed.

Introduction

On July 16, 2020, the Court of Justice of the European Union (CJEU), in *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* (*Schrems II*), invalidated the Privacy Shield that had provided a mechanism for data transfers between the United States and Europe.[1] Over 5,300 companies relied on the Privacy Shield to facilitate transatlantic data transfers for services including social media, messaging, cloud services, and email.[2] The Privacy Shield enabled these companies to freely transfer data between markets, thereby permitting them to sell physical and digital goods and services to consumers in Europe. Recent figures indicate that these commercial activities made up a significant portion of the over $7 trillion in transatlantic trade that takes place every year.[3]

In the *Schrems II* case, the CJEU found that U.S. surveillance laws do not provide an adequate level of protection for the personal data of European Union (EU) citizens that is equivalent to the rights guaranteed in the EU by the General Data Protection Regulation (GDPR). The CJEU also found that the United States lacks any mechanism to provide effective and independent review and redress for EU citizens whose data is transferred to the United States. The decision has created ambiguity around the future of trade between businesses in the United States and the EU.

The United States and the EU are currently engaged in negotiations seeking to resolve the concerns presented by the CJEU. In order for the U.S. government to create an effective and sustainable solution, it must institute reforms to the U.S. surveillance ecosystem. This report puts forth recommendations for measures that the U.S. government can implement in the near term, without need for congressional action, with the aim of providing guidance for the negotiation process and meaningfully addressing the concerns set forth in *Schrems II*.

Since the CJEU's decision in *Schrems II* addresses protections for the data—and the interests—of EU citizens, meeting the court's concerns requires increasing protections for non-U.S. persons.[4] It is worth noting, however, that most of the increased safeguards that we recommend for non-U.S. persons would also increase protections for the rights of Americans. For example, proposals to institute narrower standards for surveillance targeting would result in data collection that better focuses on appropriate targets and intrudes less on the privacy of U.S. persons and non-U.S. persons alike.

We do not suggest that every measure we recommend in this report is strictly required by the *Schrems II* decision, nor can we forecast that if all of the recommendations we set forth here are adopted, this would fully satisfy the CJEU. Rather, we seek to outline a package of reforms that address the *Schrems II* decision, that increase privacy safeguards for both U.S. persons and non-U.S. persons, and that should be achievable in the near term. Although we will

continue to urge the U.S. government to adopt comprehensive surveillance reforms beyond those outlined in this report,[5] we focus here on measures that should be feasible and actionable by the U.S. Intelligence Community without need for statutory changes. In some instances, we note that legislation would be necessary to fully resolve the CJEU's concerns, and in most cases we urge that steps taken by the executive branch should subsequently be codified by Congress. We plan to elaborate on those items that require congressional action in a subsequent report.

Background on Applicable U.S. Surveillance Authorities

In the *Schrems II* decision, the CJEU found that U.S. surveillance conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and under Executive Order 12333 (EO 12333) does not provide "the minimum safeguards" required under EU law to satisfy the principle of proportionality. As a result, the court found that surveillance conducted under those two authorities "cannot be regarded as limited to what is strictly necessary."[6]

Section 702 authorizes the U.S. government to target non-U.S. persons located outside the United States for foreign intelligence purposes, in order to collect their communications, including the content of phone calls and emails. The government collects this information inside the United States, either by compelling electronic communications service providers to turn over communications to the government (often referred to as "PRISM" collection), or by collecting communications from the internet "backbone" with the compelled assistance of internet service providers (often called "upstream" collection).[7] Although U.S. persons cannot be targeted under Section 702, their communications may be collected through what the government calls "incidental collection," if, for example, they are on the other end of an email or phone call with a target. The U.S. government must obtain annual approvals from the FISA Court—a special court that operates in secret to review classified information—for Section 702 surveillance. The FISA Court reviews and approves "certifications," which cover the categories or topics of surveillance that are authorized, as well as targeting procedures, minimization procedures, and querying procedures.

EO 12333 is an executive order originally issued by President Ronald Reagan that governs most U.S. Intelligence Community activities. It provides a framework for surveillance that is not covered by FISA, as well as for intelligence collection through other methods such as human intelligence and geospatial intelligence. Each component of the Intelligence Community has developed its own set of applicable implementing rules under EO 12333. These procedures, which must be approved by the U.S. attorney general, are also referred to as AG guidelines.[8] The lead intelligence agency for conducting signals intelligence, or SIGINT (the type of intelligence collected through surveillance), is the National Security Agency (NSA). Because the NSA sits within the Department of Defense (DoD), DoD's AG guidelines, found in DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*,[9] as well as the SIGINT Annex to these procedures,[10] provide the applicable rules for most surveillance conducted under EO 12333.

In addition, signals intelligence conducted under EO 12333 is governed by Presidential Policy Directive 28 (PPD-28), which was issued by President Barack

Obama in January 2014. PPD-28 was designed to provide safeguards for the data and rights of non-U.S. persons. However, the CJEU in *Schrems II* found that PPD-28 is not sufficient to overcome the privacy threats to EU citizens' data that it identified from U.S. surveillance conducted under both Section 702 of FISA and EO 12333.

Reforms to Collection and Targeting

Collection of information is the first step in conducting surveillance, and the first point at which government actions interfere with the privacy interests of individuals. Reforms that would address collection and targeting practices under Section 702 and EO 12333 would limit the risk of intrusion on the privacy rights of both non-U.S. persons and Americans, and would likely be the most effective means of protecting those rights. Specifically, narrowing definitions for how surveillance may be targeted and raising the standards for approving particular targets will reduce privacy threats because surveillance will focus more closely on appropriate targets. Such measures can also improve the efficacy of surveillance activities by assisting intelligence agencies in honing in on actual threat actors and actionable intelligence.

Reforms that would address collection and targeting practices … would limit the risk of intrusion on the privacy rights of both non-U.S. persons and Americans, and would likely be the most effective …

Limiting Bulk Collection Under EO 12333

Bulk collection, which involves conducting surveillance without any defined target or other "discriminants"—characteristics that define or limit—is not permitted under Section 702. However, for foreign intelligence collection under EO 12333, the U.S. government does assert the authority to conduct bulk collection when it is "necessary" to collect signals intelligence in bulk due to "technical or operational considerations."[11]

Since, by definition, bulk collection is conducted without discriminants, it creates significant risks that the government will also acquire vast quantities of information concerning people who have no connection with wrongdoing or foreign intelligence information. The U.S. government can and should implement robust safeguards to mitigate these risks, and the executive branch can adopt such measures without any action by Congress. Because both EO 12333 and PPD-28 were issued as executive actions, the president has full authority to

expand the protections for individual rights under them by issuing a new executive order or policy directive. The U.S. government can also develop and issue updated attorney general–approved guidelines.

At present, Section 2 of PPD-28 provides some limitations on bulk surveillance and protections for non-U.S. persons' data by requiring that intelligence agencies may only use signals intelligence collected in bulk for six designated purposes. The permitted categories are the purposes of detecting and countering threats from or regarding: (1) espionage; (2) terrorism; (3) weapons of mass destruction; (4) cybersecurity; (5) U.S. or allied armed forces; and (6) transnational criminal acts.[12] However, not only are these categories relatively broad but they only govern the *use* of data collected in bulk and do not in any way limit the purposes for which data may be *collected* in bulk in the first place. In other words, intelligence agencies are still permitted to 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.

Thus, as an initial reform, the U.S. government should build upon PPD-28 by applying the six-category *use* limits for bulk data to cover the purposes for bulk *collection*. No bulk collection should be permitted for any other purposes.

In addition, 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 principles 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.[13] In December 2020, the Organization for Economic Co-operation and Development's Committee on Digital Economy Policy, which includes the United States as a member,[14] issued a statement explaining the need for an instrument setting out principles for government access to personal data held by the private sector. The statement noted that these principles may include requirements that government access must "meet legitimate aims and be carried out in a necessary and proportionate manner."[15]

Current rules in the SIGINT Annex, which, as noted above, essentially govern most signals intelligence collection under EO 12333, contain the seeds for such necessity and proportionality limits. With regard to necessity, Section 2.2(a)(2) already states that the government should use discriminants whenever practicable and that bulk collection may be used "when necessary due to technical or operational considerations." For proportionality, Section 2.3(a) states that the government should endeavor "to limit the types and aspects of the information collected to those relevant to the purposes of the collection."[16] The intelligence agencies are also already familiar with the "least intrusive means"

standard,[17] which is similar to the proportionality principle but framed as only permitting certain collection methods when no less intrusive means are available. The U.S. government should build on this foundation to clearly require implementation of the necessity and proportionality principles.

Strengthening and Narrowing Justifications for Targets of Surveillance

With regard to surveillance that is not considered bulk collection, the intelligence agencies should narrow the scope of collection to better focus on legitimate targets. There are several approaches that could help in this regard under both Section 702 and EO 12333. These include narrowing the definition of foreign intelligence information that may be sought through surveillance, and strengthening the standards for what agents must show in order to justify particular surveillance targets.

Both FISA Section 702 and EO 12333 allow for broad targeting due to their sweeping definitions of what constitutes "foreign intelligence." The expansive FISA definition of foreign intelligence information includes such matters as those relating to the national defense and foreign affairs of the United States. EO 12333 defines "foreign intelligence" even more broadly as information "relating to the capabilities, intention or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists," and thus includes information that simply relates to the activities of "any foreign person."[18]

Under Section 702, targets can be any non-U.S. person, regardless of that person's level of connection to a foreign power.[19] The targeting procedures require that the surveillance of the target must be likely to lead to the collection of foreign intelligence information within the scope of one of the "certifications" or topics for which surveillance has been approved by the FISA Court—such as counterterrorism or weapons of mass destruction. This standard could permit targeting of people who may unwittingly or unknowingly possess information that meets the broad definition of "foreign intelligence." The rules for selecting non-U.S. person targets under EO 12333 are even more permissive; the government must have a valid foreign intelligence purpose for its collection, but there are no further limits on selecting non-U.S. persons as targets for surveillance.

While it is unclear whether the intelligence agencies use these authorities quite as expansively as their language appears to allow, the definitions here should be narrowed to strengthen safeguards for the data of both foreign persons and U.S. persons.

The government can implement these improved protections in the near term without need for congressional action. As noted above, no changes to EO 12333 would require legislation. Moreover, under Section 702, the government can incorporate new limits into its targeting procedures at the time of its next annual renewal of the 702 program, which the FISA Court can then approve. Such a move would be binding and narrow the government's collection. Subsequently, Congress could codify limits to ensure they are made permanent.

First, the government should commit—in its Section 702 targeting procedures—to following the definition of foreign intelligence information under FISA that applies to U.S. persons, namely that information must be "necessary to" the United States' ability to protect against threats, rather than the broader "relates to" standard that applies to foreign intelligence information regarding non-U.S. persons.[20] Further, the government should strengthen and narrow the standard for targeting under Section 702 from "reasonably likely to return" foreign intelligence information related to one of the 702 certifications. Restricting targeting to foreign powers or agents of a foreign power (as under other sections of FISA), as some have proposed, may be too limiting, but the Intelligence Community should work with reform advocates and the administration to develop narrower but workable limits.

Relatedly, the U.S. government should commit that it will not reinstate "about" collection under Section 702, ensuring that the NSA only collects communications that are "to" or "from" a target. As part of its "upstream" surveillance under Section 702, the NSA used to collect communications that merely reference, or are "about," a target, such as when the email address for a target appears in the body of an email. "About" collection therefore could sweep up communications that are neither to nor from an approved target, creating a significantly greater risk of including the communications of people with no connection to wrongdoing or foreign intelligence. The NSA suspended "about" collection in 2017 based on its inability to conduct this collection in compliance with applicable privacy protections,[21] but the statute permits the NSA to restart "about" collection after obtaining permission from the FISA Court and notifying Congress. Again, to guarantee a more permanent limit on overbroad surveillance, Congress should also pass a reform bill that includes a prohibition against "about" collection.

With regard to EO 12333, simply removing "foreign persons" from the definition of foreign intelligence would ensure that collection is limited to information regarding foreign governments, organizations, and terrorists, rather than any foreign individual. This can be done through administrative action, including a new directive or executive order. Currently, collection must be supported by a "foreign intelligence" purpose, but there are no standards to ensure that agents have a sufficient predicate for concluding that particular targets will fulfill the foreign intelligence purpose. The standard for surveillance targeting under EO 12333 should at the very least be elevated to the Section 702 targeting standard of

"reasonably likely to lead" to foreign intelligence, and could be strengthened further by working with the Intelligence Community, as suggested above.

Requiring Post Hoc Judicial Review of Targeting Decisions

Independent judicial review provides a fundamental safeguard for civil liberties. As noted above, under Section 702, the FISA Court only reviews the government's annual "certifications" for the categories of surveillance that will be permitted, together with the government's targeting, minimization, and querying procedures. The FISA Court reviews these submissions on an annual basis and, in between annual reviews, will only consider particular compliance incidents that are brought to the court's attention. The court does not play any role in reviewing the government's selection of particular targets. And for signals intelligence conducted under EO 12333, no court plays any role in assessing targeting procedures or determinations of particular targets.

In the near term, the U.S. government should seek and create procedures for FISA Court review of targeting decisions under Section 702, at least after the fact as part of the annual review of the Section 702 program. This would provide a critical independent check on targeting decisions to help ensure that they meet all applicable standards and to promote compliance. In its 2014 report on Section 702 surveillance, the Privacy and Civil Liberties Oversight Board (PCLOB) recommended that the government submit a random sample of 702 targeting decisions to the FISA Court for review as part of the annual certification process. [22] The government provided the FISA Court with a briefing on how this could work, but the FISA Court itself declined to accept the recommendation.[23] To ensure post hoc review by the FISA Court of a selection of targeting decisions, the government should build such a process into its targeting procedures as part of its submission to the FISA Court at the next annual renewal of the Section 702 certifications. The government should update its 702 targeting procedures to outline that, in order to ensure compliance, the government will submit a random sample of targeting decisions to the FISA Court for post hoc review, and specify the sampling methodology to be used.

In the longer term, Congress should enact a requirement for such post hoc FISA Court review of targeting decisions. This would provide a more fail-safe mechanism to ensure that the FISA Court would accept jurisdiction to review Section 702 targeting decisions, and Congress could expand the post hoc review to cover all targets approved in the prior year rather than only a random sample.[24] To the extent that such reviews substantially increase the workload of the FISA Court, Congress should also ensure that the FISA Court has sufficient resources to take on this work, possibly including expanding the number of judges serving on the FISA Court.[25] Congress could also authorize the FISA Court to conduct post hoc review of targeting under EO 12333 to ensure that such targeting meets

the necessity and proportionality principles. Any judicial role in intelligence collection conducted pursuant to EO 12333 would be a significant change, and therefore it would also be critical to expand resources to the FISA Court and to establish appropriate procedures.

Minimization Reforms

Minimization is the broad term that covers how the intelligence agencies may access, use, retain, and share collected data. Section 702 requires the government to adopt minimization procedures "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[26] The minimization procedures must be approved by the FISA Court on an annual basis. Each participating intelligence agency has adopted its own Section 702 minimization procedures, which generally include use limitations, retention limits, and rules regarding dissemination or sharing of information.

Collection and minimization under EO 12333 are governed by rules promulgated by the federal intelligence agencies and approved by the attorney general. As noted above, because the NSA sits within the DoD, the minimization procedures for most signals intelligence under EO 12333 are found in DoD Manual 5240.01,[27] as well as the SIGINT Annex.[28]

Strengthening Use Limitations

Throughout the *Schrems II* decision, the CJEU refers to the U.S. intelligence agencies' "mass processing" of EU citizens' personal data as an infringement upon GDPR, which suggests that use limitations could be helpful in mitigating its concerns. Therefore, the U.S. government should adopt more robust and transparent limits on how collected information regarding specific individuals—regardless of nationality—may be used. For example, for data collected under EO 12333, the government should restrict *all* use of non-U.S. persons' information to the six purposes laid out for bulk collection under PPD-28, as described above. For information collected under Section 702, the intelligence agencies should only be permitted to use information in connection with the approved foreign intelligence purpose—namely the subject of the particular certification approved by the FISA Court—for which it was collected.

Raising the Bar for Queries Using Identifiers Associated with Non-U.S. Persons

One of the key techniques that the Intelligence Community employs to review and analyze collected signals intelligence is to conduct "queries." This process involves inputting search terms into digital tools that will then comb through, or "query," the applicable databases to locate information containing the search terms. Query terms may be based on a particular subject matter, but often the

terms involve identifiers that are associated with a particular person. When query terms relate to a specific U.S. citizen or legal permanent resident, the Intelligence Community refers to the process as conducting a "U.S. person query," and there are rules that govern both the standard and the process for conducting such queries. However, most of these rules do not apply to non-U.S. person queries.

Under Section 702, the querying procedures for both the NSA and the Central Intelligence Agency (CIA) provide that all queries, regardless of the search terms used, "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, unless otherwise specifically excepted in these procedures."[29] The Section 702 querying procedures of the Federal Bureau of Investigation (FBI) add an additional permissible purpose of reasonably likely to retrieve "evidence of a crime."[30] For U.S. person queries, there are also certain procedural requirements designed to impose some rigor to the process. When either the NSA or CIA seeks to conduct a U.S. person query, the agent must produce "a statement of facts showing that the use of that query term" will be reasonably likely to return foreign intelligence information. For the NSA, the procedures also require that any U.S. person query term must first be approved by the NSA's Office of General Counsel, and such approvals will expire after one year unless they are renewed during that time. The FBI's querying procedures are somewhat more complicated but generally require that the FBI produce a statement of facts showing that the query term meets the standard before an agent may review information returned from conducting a U.S. person query. In some limited circumstances, the FBI must obtain an order from the FISA Court before they access the information.[31]

By contrast, when any of these agencies conduct Section 702 queries using terms associated with a particular non-U.S. person, there are no similar documentation or process requirements. For non-U.S. person queries, no agency is required to prepare a written statement of facts showing that the query meets the "reasonably likely to return" standard. Nor is there any requirement, like the one the NSA applies for U.S. person query terms, for prior approval of non-U.S. person query terms.

Under EO 12333, the DoD procedures include a high-level purpose requirement, namely that agents may only conduct queries that are "relevant to the intelligence mission or other authorized purposes."[32] Although this language is contained within a section outlining protections for U.S. person information, its broad drafting suggests that this purpose requirement arguably applies to all queries. Moreover, the CIA may also collect electronic communications information, and its rules under EO 12333 require that any query of unevaluated information must be "reasonably designed to retrieve information related to a duly authorized activity of the CIA."[33]

As with Section 702, there are more rigorous requirements for U.S. person queries of information acquired under EO 12333 than for other queries. For U.S. person

queries, the DoD manual also requires that queries should be designed to minimize the amount of non-pertinent information returned, and that agencies should develop procedures for documenting the basis for such queries.[34] In addition, the SIGINT Annex contains specific limits on conducting U.S. person queries, and permits such queries only if one of a list of conditions is met. These include that the query subject has been approved as a target of surveillance under FISA, and procedures also outline certain circumstances under which approval must be received from the director of the NSA or the U.S. attorney general in order to conduct a U.S. person query. By contrast, beyond the broad "relevant to an authorized purpose" rule, the DoD procedures and SIGINT Annex do not contain any specific requirements for queries using terms associated with a specific non-U.S. person, unless that individual is physically present in the United States.

Queries are a critical tool through which U.S. intelligence agencies process data, and processing safeguards for non-U.S. persons are direly needed.

There has been a significant amount of debate in the United States over strengthening the standards for when it is permissible to conduct U.S. person queries, and it is still critical that the government strengthen those standards.[35] But, to respond to the *Schrems II* decision, the U.S. government should also raise the bar for queries seeking information about residents of other countries. Queries are a critical tool through which U.S. intelligence agencies process data, and processing safeguards for non-U.S. persons are direly needed.

At a minimum, under Section 702, the U.S. government should extend the requirement for a supporting statement of facts to cover all queries seeking information about any specific person, regardless of that person's nationality or location.[36] As noted above, NSA and CIA personnel are already required to document the basis for their U.S. person queries, and the government should expand application of this rule to all agencies participating in Section 702 and to non-U.S. person queries. The rationale for mandating documentation is that it induces agents to think through, and support with facts, their assessment that using the query term will actually meet the query standard. A requirement for a statement of facts in support of query terms will therefore help ensure that queries actually meet the standard—"reasonably likely to return" foreign intelligence information—that already applies to all queries under Section 702.

Further, the U.S. government should apply this same standard and documentation requirement to queries of SIGINT data collected under EO 12333, whenever the query uses a term associated with a specific person, regardless of nationality. This will help ensure that all queries of surveillance data collected under EO 12333 are designed to be reasonably likely to return foreign intelligence information.

Decreasing Retention Periods

The privacy rights of both U.S. and non-U.S. persons can also be improved by addressing the data retention policies that apply to information gathered by the intelligence agencies. Generally speaking, the privacy risks increase the longer a piece of information is held. If some data has been deleted, it obviously cannot thereafter be inappropriately accessed or misused. This is why it is important for standard retention periods to be no longer than is necessary to serve the purpose for which the data was collected. Although intelligence agencies assert that they never know when a piece of information may turn out to be helpful, default retention periods for data that has not been identified as relevant to foreign intelligence purposes should be shortened. Agencies should have an obligation to review collected intelligence information and determine what data meets retention standards and what data can and should be purged, in a timely manner.

The default retention period for data collected by the U.S. government under both Section 702 and EO 12333 is five years in most cases.[37] The FBI is authorized to retain Section 702 data for up to 15 years in certain circumstances and with some additional safeguards.[38] In general, data that has been identified as "foreign intelligence" can be retained indefinitely, but data that has not been reviewed, or has been reviewed but not identified as foreign intelligence information, will age off at the end of the default retention period. Lowering the default time period to three years under both authorities will better protect personal data by removing it from the government's systems faster. In at least one context, government officials have already found that a three-year retention period for surveillance information is sufficient to preserve data during its period of maximum effectiveness.[39] Moreover, it is important to recognize that decreasing the default retention period does not prevent the intelligence agencies from retaining information indefinitely when they have already assessed that the particular data constitutes foreign intelligence information.

In addition, each agency's Section 702 minimization procedures contain exceptions to the default retention rule that should be examined and narrowed. For example, most of the agencies have exceptions for encrypted information or for information necessary to pursue the broadly stated "authorized foreign intelligence or counterintelligence requirements."

Further, when intelligence agency personnel actually review collected information and do not affirmatively assess it to qualify as foreign intelligence information, they should be required to purge that data rather than waiting until expiration of the default retention period. Disturbingly, the FBI's Section 702 minimization procedures actually take the opposite approach—if information has been reviewed but "*not* identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime," this is still sufficient to extend the default retention period to 10 years or, with certain additional controls in place, up to 15 years.[40] By contrast, the NSA's Section 702 minimization procedures state that they require purging data regarding U.S. persons "at the earliest practicable point" at which the NSA can determine that the information is "clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime."[41] Purging data that does not qualify as foreign intelligence information can be a critical safeguard for civil liberties.[42] However, the NSA's rule only applies to information regarding U.S. persons and, in practice, "most collected communications are not reviewed for the purging of non-foreign intelligence matters upon collection, or at any set time thereafter prior to use."[43]

We recognize that significant quantities of information will likely not be reviewed before the data ages off under the applicable default retention period. However, when intelligence analysts or agents actually review collected information, they should be required to make a determination as to whether or not the data qualifies as foreign intelligence information that the agency is authorized to retain. Any information that does not meet the applicable standard should be purged. This purge requirement should apply to all collected information that fails to qualify as foreign intelligence information (or, for the FBI, as evidence of a crime), regardless of the nationality of the person who is the subject of the information. The FBI's and CIA's procedures should be amended to incorporate an obligation to assess the value of information when conducting a review of collected data. The minimization procedures for all intelligence agencies participating in the Section 702 program should also be updated to reflect the purging requirement, and it should be fully enforced, for both U.S. and non-U.S. persons, with proper oversight.

In addition, the FBI's broad authorization for 10- and 15-year default retention periods should be eliminated. Information that has been assessed to constitute foreign intelligence information or evidence of a crime may already be retained beyond the default period. If the FBI seeks to extend the retention period for any information not yet assessed to meet this standard, the FBI should be required to make a showing to the FISA Court demonstrating the reason why longer retention periods for this data—which has not been assessed to constitute foreign

intelligence or evidence of a crime—is necessary, and how the longer retention period will meet the authorized purpose for the data collection.

Improving Transparency

Currently, the U.S. Intelligence Community discloses some data that outlines the scope and scale of their intelligence collection efforts. For example, the Office of Civil Liberties, Privacy, and Transparency of the Office of the Director of National Intelligence (ODNI) publishes its annual *Statistical Transparency Report Regarding Use of National Security Authorities*, which features data on FISA probable cause court orders and targets; FISA Section 702–related orders, targets, and U.S. person queries; national security letters; and more.[44] Most of the data in the ODNI's annual transparency report is disclosed based on legal requirements in FISA. However, the ODNI report also includes some data points whose disclosure is not mandated by FISA. FISA also requires the government to submit further reports to Congress, but much of this information remains classified and therefore unavailable to the public.

Companies that receive requests for user data from the government, such as technology and telecommunications companies, also publish some data around the requests they receive. This has become an industry-wide best practice for technology companies.[45] However, these platforms face constraints around what kind of data they can report on. In particular, companies that receive demands for customer data under FISA can only report statistics describing the type and number of demands they receive on an aggregated basis, using specified numerical bands such as 0 to 499 and 500 to 1,000.[46]

Greater transparency for the rules governing U.S. surveillance and the scope and scale of data collection would help promote accountability, and provide a check to show that collection is proportionate to intelligence needs. In particular with regard to collection under Section 702, the government should disclose the categories that are the subjects of the certifications approved by the FISA Court. Thus far, the Intelligence Community has disclosed that these subjects include counterterrorism and addressing weapons of mass destruction, but they have not declassified the full list of categories covered by the Section 702 certifications.

While greater transparency is needed[47] and will benefit U.S. and non-U.S. persons alike, it is important to note that any transparency measures should serve as a supplement to efforts to reform collection, targeting, and minimization rules. Transparency mechanisms alone will not be enough to satisfy the CJEU's concerns.

Creating Meaningful Redress

In the *Schrems II* decision, the CJEU specifically pointed to the fact that "EU citizens do not have the same remedies in respect of the processing of personal data by the US authorities" due to the Fourth Amendment not applying to them, and made clear that individuals must have access to judicial remedies to challenge interference with their rights. Targets of U.S. surveillance under Section 702 and EO 12333, including EU citizens, lack a mechanism through which they can seek redress in U.S. courts. 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." EO 12333 is particularly problematic for both U.S. and non-U.S. persons, because, as the court noted, "the NSA's activities based on E.O. 12333 are not subject to judicial oversight and are not justiciable."

The CJEU explained that an effective method of judicial redress is particularly significant to protecting EU citizens' rights, and it laid out a number of key requirements. First, to offer essential equivalence to Article 47 of the EU Charter of Fundamental Rights, effective judicial redress requires that individuals are entitled to hearings before an independent and impartial tribunal.[48] Further, the CJEU wrote that legal remedies must offer individuals access to their obtained personal data, and the ability to obtain the rectification or erasure of such data.[49] The CJEU specified that the appointment of a Privacy Shield ombudsperson (an individual within the U.S. State Department to whom individuals could raise concerns, which was a U.S. solution following *Schrems I*) did not solve the problem because that ombudsperson could not be considered an independent tribunal and lacked the ability to make decisions that would be binding upon intelligence agencies.[50]

Accordingly, in order to reinstate data flows between the United States and the EU, one crucial fix will be to provide EU citizens with a mechanism for independent judicial redress. To fully meet the redress standard set forth by the CJEU, legislation will be needed. Proposals for administrative solutions may be worth considering and could be a helpful first step to show good faith in negotiations, but ultimately Congress will need to provide a judicial redress mechanism through legislation in order to meet the robust standards the CJEU has set. Providing an independent tribunal with fact-finding ability will require jurisdiction in U.S. courts, which must be established by statute. Similarly, legislation will be required 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 —to bring challenges to surveillance practices in U.S. courts.

Academics have developed a creative proposal that attempts to meet the CJEU's robust requirements through reforms that would only require administrative action, without any legislation.[51] That proposal involves establishing a fact-finding process that can examine classified information, whose findings could then be appealed to an independent judicial body. Under the first step of the proposal, agencies that conduct or assess surveillance would be required to carry out fact-finding investigations regarding that surveillance—either through intelligence agency privacy and civil liberties officers,[52] the PCLOB, or potentially through agency inspectors general.[53] The authors of this proposal suggest that complainants who were not satisfied with the fact-finding could then obtain review in the FISA Court without need for legislation, at least for challenges related to Section 702 surveillance. They contend that the FISA Court would have jurisdiction as part of its authority to review compliance incidents. The authors further suggest that Congress could enact legislation to grant complainants standing to file appeals in the same way as under the Freedom of Information Act (FOIA), where individuals who are not satisfied with an agency's response to a FOIA request always have standing to seek judicial review of the agency's investigation. The authors see this review as analogous to judicial review of other agency actions under the Administrative Procedures Act (APA).

... but ultimately Congress will need to provide a judicial redress mechanism through legislation in order to meet the robust standards the CJEU has set.

While the purely administrative version of this proposal could help serve as an interim solution, it is highly unlikely that it would suffice as a longer-term redress fix. One issue is that the potential fact finders considered do not have the power to require the intelligence agencies to act and, as noted above, the CJEU found that the redress mechanism must be binding on the intelligence agencies to "remedy the deficiencies" in the law.[54] If the PCLOB were tasked with the initial fact-finding investigations under this type of proposal, this would offer more independence than either an intelligence agency's privacy and civil liberties officer or a State Department official (as with the Privacy Shield ombudsperson). But the PCLOB would then need additional authority, which would ultimately require congressional action to require compliance with their decisions. Further, it is far from clear that, without legislation, the FISA Court would agree that it had jurisdiction to review appeals from the proposed fact-finding investigations as part of its review of compliance matters. By definition, a complainant would

only seek to appeal an agency fact-finding where the fact-finding process had concluded that there was *not* a compliance violation, so such determinations may not fit within the scope of reviewing compliance violations that the FISA Court recognizes to be under its jurisdiction. Moreover, the FISA Court does not review decisions of the PCLOB or inspectors general. Therefore, if either of those actors handled the proposed fact-finding process, the FISA Court would likely be unable to assert jurisdiction without legislative authorization. In addition, even if the FISA Court accepted review as part of the compliance process, this could only provide redress related to Section 702; the FISA Court does not have jurisdiction to review any activities under EO 12333, and therefore legislation would still be required to create a mechanism for redress under EO 12333.

Under current law, there are a variety of barriers not only for Europeans but also for Americans who seek to challenge U.S. surveillance practices in U.S. courts. In particular, such challenges have been blocked by the inability of plaintiffs to establish standing—because without access to classified information, they cannot show that they have been subject to surveillance. However, the U.S. Supreme Court has held that Congress can play a role in determining what qualifies as an "injury" that can establish standing,[55] and Congress can and should pass legislation that would more clearly define what constitutes an injury in cases challenging government surveillance. Under one proposal, Congress could provide that where a person takes objectively reasonable protective measures in response to a belief that they are subject to surveillance, those protective measures would count as the injury, and they would therefore be able to establish standing to pursue a case against the U.S. government for illegal surveillance.[56]

It seems unavoidable that legislation will ultimately be needed to provide Europeans with individual, independent redress as the CJEU laid out. Nonetheless, it is worth exploring administrative solutions in the near term to improve upon existing mechanisms, including the Privacy Shield ombudsperson, that the CJEU has rejected for failure to provide the requisite independent tribunal to ensure protections of Europeans' rights.

Conclusion

In *Schrems II*, the CJEU made clear that reforms to U.S. surveillance law are critical to ensuring future transatlantic data flows. The decision has provided an opportunity for U.S. policymakers to reexamine U.S. surveillance law and implement meaningful changes that increase privacy protections for non-U.S. persons and Americans alike. The recommendations outlined in this report are designed to accomplish these goals and should be achievable in the near term without congressional action. However, as noted throughout this report, Congress likely must enact legislation to fully resolve the CJEU's concerns and institute changes that are more robust and permanent. We plan to elaborate on those long-term reforms that require congressional action in a subsequent report.

Notes

1 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems,* C - 311/18, Court of Justice of the European Union, July 16, 2020, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN

2 Daniel Stoller, "U.S. Companies Scrambling After EU Data Transfer Pact Dies," *Bloomberg Law*, July 16, 2020, https://news.bloomberglaw.com/tech-and-telecom-law/u-s-companies-left-scrambling-after-eu-data-transfer-pact-dies

3 "EU-US Privacy Shield for data struck down by court," *BBC News*, July 16, 2020, https://www.bbc.com/news/technology-53418898

4 U.S. persons are U.S. citizens and legal permanent residents.

5 Sharon Bradford Franklin, "Statement on Behalf of OTI to the Privacy and Civil Liberties Oversight Board," New America, August 31, 2020, https://www.newamerica.org/oti/testimonies/statement-behalf-oti-privacy-and-civil-liberties-oversight-board-exercise-authorities-under-foreign-intelligence-surveillance-act/

6 Schrems II, *supra* note 1, at ¶ 184.

7 Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014) at 32-41, https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

8 For a general overview of E.O. 12333 and what it covers, *see* Privacy and Civil Liberties Oversight Board, *Executive Order 12333* (2021) https://documents.pclob.gov/prod/Documents/OversightReport/4f1d0d87-233b-4555-9b87-79089ad9845e/12333%20Public%20Capstone.pdf. The Office of the Director of National Intelligence (ODNI) has posted a chart with links to the current A.G. Guidelines for each intelligence agency, available at https://www.intel.gov/assets/documents/guide/Chart_of_EO_12333_AG_approved_Guidelines_March_2021.pdf.

9 DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 2016 https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887

10 Signals Intelligence Annex to DoD Manual S-5240.01-A, 2021, https://www.nsa.gov/Portals/70/documents/about/civil-liberties/resources/Redacted%20Annex%20DODM%20S-5240.01-A.pdf

11 Presidential Policy Directive 28: Signals Intelligence Activities, January 17, 2014, at n. 5, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities; Signals Intelligence Annex to DoD Manual S-5240.01-A at Sec. 2.2(a)(2), https://www.nsa.gov/Portals/70/documents/about/civil-liberties/resources/Redacted%20Annex%20DODM%20S-5240.01-A.pdf

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

13 *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/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsjYoiCfMKoIRv2FVaVzRkMjTnjRO%2Bfud3cPVrcM9YR0iW6Txaxgp3f9kUFpWoq%2FhW%2FTpKi2tPhZsbEJw%2FGeZRASjdFuuJQRnbJEaUhby31WiQPl2mLFDe6ZSwMMvmQGVHA%3D%3D; Electronic Frontier Foundation, *Necessary & Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance* (2014), https://www.ohchr.org/

documents/issues/privacy/electronicfrontierfoundation.pdf.

14 OECD COMMITTEE ON DIGITAL ECONOMY POLICY (CDEP), https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=1837&Lang=en

15 "Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy," OECD, December 22, 2020, http://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

16 Signals Intelligence Annex to DoD Manual S-5240.01-A, https://www.nsa.gov/Portals/70/documents/about/civil-liberties/resources/Redacted%20Annex%20DODM%20S-5240.01-A.pdf

17 See, e.g., CIA Procedures Approved by the Attorney General Pursuant to Executive Order 12333, 2017, at Section 4.1, https://www.cia.gov/static/54871453e089a4bd7cb144ec615312a3/CIA-AG-Guidelines-Signed.pdf

18 50 U.S.C. § 1801(e); Exec. Order 12,333 at § 3.5(e), 46 FR 59941 (1981).

19 50 U.S.C. § 1881(a).

20 50 U.S.C. § 1801(e).

21 "NSA Stops Certain Section 702 'Upstream' Activities," press release, National Security Agency, April 28, 2017,https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/.

22 Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance* Act, 2014, at 141, https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

23 Privacy and Civil Liberties Oversight Board, *Recommendations Assessment* Report, 2016, at 19, https://documents.pclob.gov/prod/Documents/OversightReport/b1accb9f-0469-46f1-b660-b66acfbc601a/Recommendations_Assessment_Report_20160205.pdf

24 In 2019, the most recent year for which statistics are available, the number of approved Section 702 targets jumped to 204,968, up from 164,770 in calendar year 2018. Office of the Director of National Intelligence, Statistical Transparency Report Regarding the Use of National Security Authorities for 2019, at 14 https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf Since this is a large number, Congress would likely need to increase resources to the FISA Court in order to permit post hoc review of all Section 702 targets. Further, with a review of all targets, it would then be appropriate for the targeting procedures to require purging of any information collected from improper targeting decisions.

25 At present, there are eleven judges on the FISA Court. 50 U.S.C. § 1803(a)(1).

26 50 U.S.C. § 1801(h).

27 DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 2016, https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887

28 Signals Intelligence Annex to DoD Manual S-5240.01-A, https://www.nsa.gov/Portals/70/documents/about/civil-liberties/resources/Redacted%20Annex%20DODM%20S-5240.01-A.pdf

29 NSA Querying Procedures Pursuant to Section 702 (September 17, 2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Querying_17Sep19_OCR.pdf; CIA Querying Procedures Pursuant to Section 702 (September 17, 2019), https://www.intelligence.gov/

assets/documents/702%20Documents/declassified/2019_702_Cert_CIA_Querying_17Sep19_OCR.pdf

30 FBI Querying Procedures Pursuant to Section 702 (September 17, 2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Querying_17Sep19_OCR.pdf

31 FBI Querying Procedures, Section 4(A), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Querying_17Sep19_OCR.pdf

32 DoD Manual 5240.01, Section 3.3(f)(1)(b)(1), https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887

33 The particular section of the CIA Rules that applies will depend on how the CIA acquired the data, but this purpose standard for queries is the same. CIA Attorney General Procedures, Section 6.2.3 (data subject to exceptional handling requirements), Section 6.3.4 (data subject to routine handling requirements) https://www.cia.gov/static/54871453e089a4bd7cb144ec615312a3/CIA-AG-Guidelines-Signed.pdf

34 DoD Manual 5240.01, Section 3.3(f)(1)(b), https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887

35 Sharon Bradford Franklin, "What Happened at the Court: The Hasbajrami Oral Argument on Section 702 of FISA and the Fourth Amendment," *Just Securit y*, August 29, 2018,https://www.justsecurity.org/60505/happened-court-hasbajrami-oral-argument-section-702-fisa-fourth-amendment/

36 This recommendation for documentation does not cover queries based on subject matter or other terms that are not associated with any particular person.

37 CIA Minimization Procedures Pursuant to Section 702 (September 17, 2019), section 2(a), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_CIA_Minimization_17Sep19_OCR.pdf ; FBI Minimization Procedures Pursuant to Section 702 (September 17, 2019), section III(D)(4)(b), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Minimization_17Sep19_OCR.pdf; NSA Minimization Procedures Pursuant to Section 702 (September 17 2019), section 4(c), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Minimization_17Sep19_OCR.pdf; 50 USC §1813.

38 FBI Minimization Procedures Pursuant to Section 702 (September 17, 2019), section III(D)(4)(c), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Minimization_17Sep19_OCR.pdf

39 Privacy and Civil Liberties Oversight Board, *Repo rt on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the* Operations *of the Foreign Intelligence Surveillance Court* at 170 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf

40 FBI Minimization Procedures Pursuant to Section 702 (September 17, 2019), section III(D)(4)(c) (emphasis added), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Minimization_17Sep19_OCR.pdf

41 NSA Minimization Procedures Pursuant to Section 702 (September 17, 2019), section 4(b)(1), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Minimization_17Sep19_OCR.pdf

42 Separate Statement of Chairman David Medine and Board Member Patricia Wald, PCLOB Section 702 Report at 153 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

43 Separate Statement of Chairman David Medine and Board Member Patricia Wald, PCLOB Section 702 Report at 153 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf.

44 Office of the Director of National Intelligence, Statistical Transparency Report Regarding the Use of National Security Authorities for 2019, https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf

45 New America's Open Technology Institute, The Transparency Reporting Toolkit (Dec. 29, 2016), https://www.newamerica.org/oti/policy-papers/transparency-reporting-toolkit-reporting-guide-and-template/

46 50 U.S.C. § 1874.

47 Sharon Bradford Franklin, "Statement on Behalf of OTI to the Privacy and Civil Liberties Oversight Board," New America, August 31, 2020, https://www.newamerica.org/oti/testimonies/statement-behalf-oti-privacy-and-civil-liberties-oversight-board-exercise-authorities-under-foreign-intelligence-surveillance-act/

48 Schrems II, *supra* note 1, at ¶ 186.

49 Schrems II, *supra* note 1, at ¶ 187.

50 Schrems II, *supra* note 1, at ¶ 195 - 97.

51 Kenneth Propp and Peter Swire, "After Schrems II: A Proposal to Meet the Individual Redress Challenge," *Lawfare*, August 13, 2020, https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge

52 The Honorary Director of the European Data Protection Supervisor (EDPS) has suggested that Inspectors General within the Intelligence Community might be more appropriate given their greater independence. Christopher Docksey, "Schrems II and Individual Redress: Where There's a Will There's a Way," *Lawfare*, October 12, 2020, https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way

53 Peter Swire, "Statutory and Non-Statutory Ways to Create Individual Redress for U.S. Surveillance Activities," Appendix I to Testimony Before U.S. Senate Commerce Committee on "The Invalidation of the E.U.-U.S. Privacy Shield and the Future of Transatlantic Data Flows, "January 14, 2021, https://www.crossborderdataforum.org/statutory-and-non-statutory-ways-to-create-individual-redress-for-u-s-surveillance-activities/

54 Schrems II, *supra* note 1, at ¶ 190, 196.

55 *Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1549 (2016).*

56 Ashley Gorski, Patrick Toomey, and Kate Ruane, "The Future of U.S. Foreign Intelligence Surveillance, *Just Security*, November 11, 2020, https://www.justsecurity.org/73321/the-future-of-u-s-foreign-intelligence-surveillance/; USA Rights Act of 2017, Section 11, https://www.wyden.senate.gov/imo/media/doc/USA%20RIGHTS%20Act%20Leg%20Text.pdf

NEW AMERICA