CENTER FOR DEMOCRACY & TECHNOLOGY

Schrems II and the Need for Intelligence Surveillance Reform

January 13, 2021

This memorandum describes a series of administrative and legislative reforms to U.S. surveillance law and practice that will advance the rights of non-U.S. persons and of the U.S. persons who communicate with them. It is prepared by the Center for Democracy & Technology (CDT), a 25-year-old 501(c)(3) nonprofit organization working to promote fundamental rights and democratic values by shaping technology policy and architecture. CDT has offices in Washington, D.C. and in Brussels. We consulted with former officials of the U.S. intelligence community, academics, companies, and other civil society organizations to prepare this document. We do not purport to have all the answers: our intelligence surveillance reform agenda is a work in progress, and will be influenced by the reaction we receive to these proposals and by the ideas others share.

In short, the reforms we recommend will:

- Increase transparency about surveillance actually conducted;
- Limit the purposes for which surveillance can be conducted;
- Focus surveillance on legitimate targets;
- Require more timely deletion of information collected unnecessarily; and
- Establish a route to court-ordered redress for unlawful surveillance.

BACKGROUND

The Court of Justice of the European Union (CJEU) issued a decision in July 2020, known colloquially as the "Schrems II" decision, that struck down the Privacy Shield agreement between the European Union and the United States. Approximately 5,300 U.S. companies relied on the EU-U.S. Privacy Shield as the basis for their compliance with EU law, particularly the GDPR, when transferring personal data from the EU to the United States.

The CJEU found that Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA)[1] and U.S. Executive Order (EO) 12333[2] failed to incorporate suitable limitations and safeguards on surveillance and that even with the Privacy Shield agreement, provided inadequate protection to that data.The CJEU ruled that for transfers to continue, U.S. surveillance laws would need to provide *essentially equivalent* protections as those afforded under the GDPR (Article 45) read in light of the fundamental rights guaranteed in Articles 7, 8 and 47 of the EU Charter of Fundamental Rights.

As a result of this decision and subsequent guidance, the lawfulness of transferring personal information from the EU to the United States is in question even while such dataflows are essential to the operations of many U.S. companies. To promote the rights of Europeans and other non-U.S. persons, and ensure the continued flow of data between the U.S. and Europe, the U.S. should adopt a series of administrative and legislative reforms that address the concerns the CJEU expressed about proportionality of U.S. surveillance, and the right of redress for unlawful surveillance.

Shortcomings of Alternatives To Surveillance Reform: Although the Schrems II decision expressly invalidated only the Privacy Shield, it called into question other mechanisms for the transfer of personal data from the EU to the U.S. For example, companies can adopt Standard Contractual Clauses (SCCs) in an effort to ensure that users' data is subject to protection that is essentially equivalent to that provided under EU law. Although the decision raises the possibility that SCCs, in conjunction with supplementary measures, could provide adequate protection, it has become apparent that adequate supplementary measures may not exist under current law. For example, according to Recommendations that the European Data Protection Board released in November 2020, although companies can protect individuals' data by encrypting it end-to-end before it is transferred to a jurisdiction with inadequate data protection controls, such encryption is not sufficient when data is transferred, for example, to a partner or affiliate in the U.S. for shared business services, or to a cloud service provider that will need to access the data in the clear.

[1] Adopted in the 2008 FISA Amendments Act, Section 702 of FISA created a mechanism through which the U.S. government can compel U.S. communications service providers to disclose users' communications content and metadata, both in real time and from storage. It is a targeted collection program, overseen by the Foreign Intelligence Surveillance Court (FISA Court) and the targets must be non-U.S. persons (persons other than U.S. citizens and lawful permanent residents) outside the U.S.

[2] Adopted in 1981, Executive Order 12333 lays out the means by which the U.S. collects foreign intelligence without the ability to compel assistance from providers, and without oversight by the FISA Court. Collection programs can be targeted at non-U.S. persons abroad, or can collect communications in bulk. In 2015, CDT identified to the UN Human Rights Council five bulk collection programs carried out by the U.S. and revealed in 2013 by NSA contractor, Edward Snowden.

Companies can also localize data in Europe and refrain from transferring Europeans' data out of Europe. However, such measures can be costly and impractical to implement, may be inconsistent with business purposes, and can further contribute to the splintering of internet services, as well as the inability to offer some services in some jurisdictions as a result of restrictions on data flows.

Finally, while a successor to the EU-U.S. Privacy Shield agreement could be helpful, any such successor agreement would likely suffer the same fate as its predecessor agreements (Privacy Shield and the EU-U.S. Safe Harbor agreement) unless it is supported by significant legislative and administrative reforms to U.S. surveillance law and practice.

The Need for Speed: Swift action on surveillance reform is needed because without these reforms, data protection authorities in Europe are poised to issue orders that could shut down, limit, or alter the transatlantic data flow. Such orders may be backed by the threat of substantial penalty for non-compliance and threaten substantial economic disruption at a time when all countries are facing severe economic challenges as a result of the ongoing pandemic. It should also be noted that such orders would be detrimental to U.S. intelligence surveillance conducted for legitimate reasons: they would reduce the amount of data subject to compelled disclosure to U.S. intelligence agencies. In other words, the continuation of compelled disclosures from U.S. companies to U.S. intelligence agencies hinges on adoption of measures to protect the civil liberties and human rights of non-U.S. persons.[3] Such measures will also benefit the rights of U.S. persons whose communications and data are incidentally collected, intentionally, when they communicate with foreign surveillance targets, and when the U.S. government engages in bulk collection.

Challenges: For a number of reasons, taking swift, effective action is no easy task. The CJEU set a high bar for both prongs of its decision, the proportionality prong and the redress prong. With respect to proportionality, the CJEU observed in Schrems II: "[I]n order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what

[3] Moreover, compelled disclosure under Section 702 is subject to more protections – including FISA Court oversight and targeting requirements – than is surveillance conducted under EO 12333. When access to compelled disclosures under Section 702 is reduced, it creates pressure to use the less protective EO 12333 surveillance regime to meet intelligence requirements. This is not a good outcome for intelligence goals or for the goal of protecting human rights.

circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary." In the Schrems I decision,[4] the CJEU said that surveillance had to be for purposes that are "specific, strictly restricted, and capable of justifying the interference" with privacy rights.

With respect to redress, the CJEU in Schrems II indicated that to be adequate, a redress mechanism had to have the following attributes:

(i) the power to order a stop to unlawful surveillance;
(ii) the power to order the deletion of information unlawfully collected;
(iii) the fact-finding capability to compel disclosure of the information necessary to the exercise of such powers;
(iv) the ability to receive complaints and hold hearings at which a person can be represented; and
(v) independence and impartiality.

On the U.S. side, there are other challenges. First, the intelligence community has identified instances in which Section 702 has been used successfully against terrorism. Policy makers are likely to be hesitant to adopt changes to Section 702 or to EO 12333 surveillance that, in their view, could undermine their effectiveness. Second, the current protections in U.S. intelligence law that pertain to surveillance directed abroad extend primarily to U.S. persons' data, and to the data of persons in the U.S. regardless of citizenship. The necessary reforms require protection of a broader group of individuals. Third, U.S. courts, including the FISA Court, are the only existing mechanisms in the U.S. that could have the attributes and authorities that the CJEU deemed necessary to an adequate redress mechanism.[5] A person challenging unlawful surveillance in a U.S. court generally has to show that they have suffered "injury" sufficient to give them standing to bring a challenge. In the context of intelligence surveillance, there is generally no notice to a target or other person whose communications were obtained, and this makes it difficult to establish standing. A route must be established through which people can bring a challenge to a federal court that is consistent with the constitutional doctrine of

[4] In Schrems I, the CJEU stuck down the predecessor to the Privacy Shield, the EU-U.S. Safe Harbor Agreement.
[5] Congress would probably have to enact legislation to give the FISA Court the authority it would need to receive and act upon complaints of unlawful surveillance and FISA Court rules would need to accommodate public hearings. Article 47 of the Charter of Fundamental Rights of the European Union provides as follows: *Article 47 - Right to an effective remedy and to a fair trial*
Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

standing. Establishing a redress mechanism that is legally adequate for the purposes of EU law will require legislation.

RECOMMENDED REFORMS

Having identified the circumstances compelling the quick adoption of surveillance reforms to protect fundamental rights, and the challenges attendant to putting such reforms in place, we now turn to the specific administrative and legislative measures CDT recommends.

Administrative Measures: The U.S. should adopt the following reforms administratively, some of which could later be required by statute. Each of these measures is calculated to address the concern of the CJEU that Section 702 and EO 12333 authorize the U.S. government to conduct surveillance that is disproportionate:

- ***Transparency:*** Increase transparency about the purposes for which Section 702 surveillance is actually conducted. Section 702 surveillance can be conducted to collect "foreign intelligence information" that is broadly defined to include information that "relates to" international terrorism, sabotage, cybersecurity, WMD proliferation, hostile acts by foreign powers, and clandestine intelligence activities of foreign powers. It can also be used to collect information that relates to two "catch-alls": national security and foreign affairs. If this power were fully utilized, there could be hundreds of millions of surveillance targets, not the approximately 200,000 targets there actually are. Each year, the U.S. government seeks FISA Court approvals of secret "certifications" that set forth the purposes for which Section 702 surveillance is actually conducted. The purposes of at least two of these annual certifications – terrorism and cybersecurity – have been publicly acknowledged. The government should publicly release these certifications, or unclassified summaries of the certifications that describe the actual purposes for which Section 702 surveillance could have been engaged in during the previous calendar year. The one-year delay precludes release of more current information that could aid foreign adversaries.
- ***Scope:*** The President should issue a binding directive limiting the scope of Section 702 surveillance. The directive would permit surveillance concerning international terrorism, sabotage, cybersecurity, and WMD proliferation, and to monitor the communications of foreign powers to protect against grave hostile acts and clandestine intelligence activities, as provided in 50 U.S.C. § 1801(e)(1). This would make it so surveillance conducted for "catch-all" purposes to collect information that "relates to" national security or foreign affairs would have to be conducted

under "regular FISA" – with the approval of the FISA Court upon a finding that the target is a foreign power or an agent of a foreign power. If deemed necessary, the administration could also permit Section 702 to be used to collect information "necessary to" U.S. national security (as opposed to information that merely "relates to" national security, as is currently permitted in the national security catch-all.) The "necessary to" standard already applies to intelligence surveillance to collect national security information when the surveillance is directed at U.S. persons.

- ***Study:*** We believe that Section 702 surveillance should be directed at people who are reasonably believed to be agents of foreign powers, such as foreign governments and foreign terrorist organizations. However, imposing such a requirement is a significant step. The Administration should conduct a study to assess the operational impact of requiring an administrative determination of reasonable suspicion that any target of intelligence surveillance is a foreign power or an agent of a foreign power.
- ***Minimization:*** The President should issue a binding directive on Section 702 and EO 12333 minimization procedures that reduces the default retention period from 5 years to 3 years and that narrows the exceptions to retention after the expiration of that period.
- ***Targeting, EO 12333:*** The Administration should establish an interagency process that has the goal of modifying EO 12333 to prohibit bulk collection and to narrow the foreign intelligence purposes for which intelligence surveillance can be conducted under that EO. Under EO 12333, foreign intelligence is defined even more broadly than in FISA, and includes "information relating to the capabilities, intentions, or activities of … foreign persons."
- ***Declassification:*** The Administration should conduct a declassification review concerning EO 12333 surveillance programs and information regarding the retention, use, and dissemination of information collected under EO 12333.

Legislative Measures: The legislative measures that should be adopted to preserve transatlantic data flows must address both prongs of the CJEU's decision in Schrems II: the redress prong and the proportionality prong.

With respect to proportionality:

- ***Scope:*** Congress should enact legislation that would codify the scope of Section 702 surveillance that is described above. Thus, Congress would limit the purposes for which Section 702 surveillance could be conducted and consider codifying a

requirement of reasonable suspicion that an intelligence surveillance target is a foreign power or an agent of a foreign power, depending on the results of the study of such a requirement called for above. It should include in that legislation the purposes for which Section 702 surveillance is *prohibited*, drawing from the prohibitions in Section 1 of Presidential Policy Directive 28 (PPD-28).[6] Thus, the U.S. would be prohibited from using Section 702 to collect foreign intelligence information for the purpose of burdening dissent or for disadvantaging people based on their ethnicity, race, gender, sexual orientation or religion.

- ***Minimization:*** Congress should enact legislation that reduces the default retention period for information acquired under Section 702 and EO 12333 from 5 years to 3 years and that narrows the exceptions to retention after the expiration of that period. Congress has already legislated in this area, generally imposing a 5-year retention period even for communications collected under EO 12333.[7]
- ***Targeting, Section 702:*** The U.S. government errantly interpreted Section 702 to permit the collection of communications that were not even to or from the surveillance target, but rather that were "about" the target. Such communications include an identifier associated with a target, such as an email address or an IP address. Some "abouts" collection was suspended in 2017 because it could not be conducted lawfully, and Congress authorized the re-start of the program, with notice to Congress, if the government resolves the operational issues. Instead, Congress should require that communications collected under Section 702 must be to or from a Section 702 target, thus outlawing "abouts" collection.

With respect to redress:

- ***Mechanism:*** Congress should enact legislation that would establish a mechanism through which individuals could seek redress in U.S. courts when intelligence surveillance has violated legal protections. This will require legislation because the existing mechanisms – such as the Privacy Shield ombudsperson, the Privacy and Civil Liberties Oversight Board (PCLOB), the Privacy and Civil Liberties Offices in the various intelligence community entities, and inspectors general – do not meet the requirement of being regarded as a tribunal within the meaning of Article 47 of the EU Charter of Fundamental Rights. According to the CJEU ruling, they lack the ability to enforce necessary safeguards and the independence of a tribunal the CJEU would

[6] PPD-28, issued by President Obama in January 2014, described limitations on intelligence surveillance conducted under EO 12333 that the government follows. A 2018 report by the Privacy and Civil Liberties Oversight Board revealed that most of the substantive requirements in PPD-28 were observed in practice by elements of the Intelligence Community prior to adoption of PPD-28.

[7] 50 U.S.C. 1813.

deem adequate. A good way to address this issue would be for Congress to enact legislation similar to Section 11 of the USA Rights Act, which Senator Wyden proposed in 2017.[8] It defined the "injury" that needs to be shown to establish standing in the surveillance context, a proper role of Congress. Persons who are likely to communicate foreign intelligence information and who take objectively reasonable measures to protect against surveillance would have the necessary "injury."

- Congress should enact legislation that would establish the circumstances in which an intelligence surveillance target would receive notice of that surveillance, including by delineating the circumstances in which information used in a legal proceeding is "derived from" intelligence surveillance for purposes of providing notice. FISA already requires that information used in a criminal proceeding that was "derived from" intelligence surveillance must be disclosed as such to the defendant.

Conclusion: The CJEU decision in the Schrems II litigation puts transatlantic data flows at risk, and raises the possibility of substantial economic disruption. At the same time, it should also be seen as an opportunity to reexamine U.S. surveillance law and practice and make necessary changes to protect the rights of people who may be subjected to such surveillance. This document identifies such changes.

For further information, contact Greg Nojeim, Director of the CDT Freedom, Security and Technology Project, gnojeim@cdt.org, or Iverna McGowan, Director of the Europe Office of CDT, imcgowan@cdt.org.

[8] https://www.congress.gov/bill/115th-congress/senate-bill/1997/text?format=txt.