UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

Letter from Deputy Assistant Secretary James Sullivan on the *Schrems II* Decision

The July 16 decision by the European Court of Justice (ECJ) in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 ("*Schrems II*") has created enormous uncertainty about the ability of companies to transfer personal data from the European Union to the United States in a manner consistent with EU law. In addition to invalidating the European Commission's 2016 adequacy decision for the EU-U.S. Privacy Shield Framework (on which more than 5,300 companies relied to conduct transatlantic trade in compliance with EU data protection rules), the ECJ's *Schrems II* ruling requires organizations that use EU-approved data transfer mechanisms like Standard Contractual Clauses and Binding Corporate Rules to now verify, on a case-by-case basis, whether foreign legal protections concerning government access to personal data meet EU standards. Accordingly, in an effort to assist organizations in assessing whether their transfers offer appropriate data protection in accordance with the ECJ's ruling, the U.S. Government has prepared the attached White Paper, which outlines the robust limits and safeguards in the United States pertaining to government access to data.

Like European nations and other countries, the United States conducts intelligence gathering activities to ensure that national security and foreign policy decision makers have access to timely, accurate, and insightful information on the threats posed by terrorists, criminals, cyber hackers, and other malicious actors. Particularly in view of the extensive U.S. surveillance reforms since 2013, however, and as detailed more fully in the White Paper, the U.S. legal framework for foreign intelligence collection provides clearer limits, stronger safeguards, and more rigorous independent oversight than the equivalent laws of almost all other countries.

While the White Paper can help organizations make the case that they should be able to send personal data to the United States using EU-approved transfer mechanisms, it is not intended to provide companies with guidance on EU law or what positions to take before EU regulators or courts. Nor does it eliminate the urgent need for clarity from European authorities or the onerous compliance burdens generated by the *Schrems II* decision.

The ECJ's ruling has generated significant legal and operational challenges for organizations around the world at a time when the ability to move, store, and process data seamlessly across borders has never been more crucial. Cross-border data flows

have become indispensable to how citizens on both sides of the Atlantic live, work, and communicate. They power the international operations and growth of American and European businesses of every size and in every industry, and underpin the $7.1 trillion transatlantic economic relationship. Most importantly, they enable governments, private companies, and organizations worldwide to leverage the data sharing and collaborative research critical to understanding the COVID-19 virus, mitigating its spread, and expediting the discovery and development of treatments and vaccines.

To address the challenges posed by the *Schrems II* ruling, the Trump Administration is exploring all options at its disposal and remains committed to working with the European Commission to negotiate a solution that satisfies the ECJ's requirements while protecting the interests of the United States. Publication of this White Paper represents an important step by our Government to help maintain the mutually beneficial flows of information that are so vital to our transatlantic partnership.

Sincerely,

James M. Sullivan
Deputy Assistant Secretary for Services
U.S. Department of Commerce

INTERNATIONAL TRADE ADMINISTRATION

Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*

White Paper

September 2020

Introduction

In its July 16, 2020 decision in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 ("*Schrems II*"), the European Union Court of Justice ("ECJ") upheld European Commission Decision 2010/87 on Standard Contractual Clauses ("SCCs") as a basis in EU law for transferring personal data to non-EU countries. The ECJ indicated that, going forward, companies relying on SCCs are responsible for determining whether the recipient country's law concerning government access to data provides privacy protections meeting EU legal standards. The ECJ in *Schrems II* also invalidated Commission Decision 2016/1250 underlying the EU-U.S. Privacy Shield. The Court found that the Commission's record underlying Decision 2016/1250 did not establish that privacy protections in U.S. law relating to intelligence agencies' access to data meet EU legal standards. Notwithstanding this finding, companies transferring data to the United States under SCCs today are responsible for undertaking their own independent analyses of all relevant and current U.S. law relating to intelligence agencies' access to data, as well as the facts and circumstances of data transfers and any applicable safeguards, in assessing whether the transfers satisfy EU law.

A wide range of information about privacy protections in current U.S. law and practice relating to government access to data for national security purposes is publicly available. The United States government has prepared this White Paper to provide a detailed discussion of that information, focusing in particular on the issues that appear to have concerned the ECJ in *Schrems II*, for consideration by companies transferring personal data from the EU to the United States. The White Paper provides an up-to-date and contextualized discussion of this complex area of U.S. law and practice, as well as citations to source documents providing additional relevant information. It also provides some initial observations concerning the relevance of this area of U.S. law and practice that may bear on many companies' analyses. The White Paper is not intended to provide companies guidance about EU law or what positions to take before European courts or regulators.

To summarize some of the key points:

(1) Most U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the ECJ in *Schrems II*.

(2) The U.S. government frequently shares intelligence information with EU Member States, including data disclosed by companies in response to FISA 702 orders, to counter threats such as terrorism, weapons proliferation, and hostile foreign cyber

activity. Sharing of FISA 702 information undoubtedly serves important EU public interests by protecting the governments and people of the Member States.

(3) There is a wealth of public information about privacy protections in U.S. law concerning government access to data for national security purposes, including information not recorded in Decision 2016/1250, new developments that have occurred since 2016, and information the ECJ neither considered nor addressed. Companies may wish to take this information into account in any assessment of U.S. law post-*Schrems II*.

Companies Not Disclosing Data to U.S. Intelligence Agencies

As a practical matter, for many companies the issues of national security data access that appear to have concerned the ECJ in *Schrems II* are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community. The ECJ examined issues arising from the concern that U.S. intelligence agencies might access transferred data under two sources of U.S. law. The first is Executive Order 12333 ("EO 12333"), a general directive organizing U.S. intelligence activities, which does not include any authorization to compel private companies to disclose data. The second is Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702"), a statute establishing a judicial process authorizing a specific type of data acquisition. Under FISA 702, an independent court may authorize the government to issue orders requiring companies in the United States to disclose communications data of specific non-U.S. persons located outside the United States to obtain specified types of foreign intelligence information. Most companies doing business in the EU do not, and have no grounds to believe they do, deal in any data that is of any interest to U.S. intelligence agencies. U.S. government commitments and public policies restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for the purpose of obtaining a commercial advantage.[1] Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data.

Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies. Neither would such companies have any indication that a U.S. intelligence agency has sought to obtain their data unilaterally

[1] *E.g.*, Presidential Policy Directive 28, "Signals Intelligence Activities" § 1(b) (17 Jan. 2014) ("PPD-28") (signals intelligence "shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose"); *id.* § 1(c) ("It is not an authorized . . . purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially"), available at link.

outside the United States under the authority of EO 12333. The theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU without the company's knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data. Moreover, this theoretical possibility exists with respect to data held anywhere in the world, so the transfer of data from the EU to the United States in particular does not increase the risk of such unilateral access to EU citizens' data. In summary, as a practical matter, companies that fall in this category have no reason to believe their data transfers present the type of data protection risks that concerned the ECJ in *Schrems II*.

Companies Relying on the GDPR's "Public Interest" Derogation

Companies transferring data from the EU that have received orders authorized by FISA 702 requiring the disclosure of data to U.S. intelligence agencies for foreign intelligence purposes may consider the applicability of the "public interest" derogation in Article 49 of the GDPR as a basis for those transfers. In *Schrems II*, the ECJ made clear that notwithstanding the invalidation of Decision 2016/1250, Article 49 derogations continue to be available for transferring personal data to the United States.[2]

The European Data Protection Board ("EDPB") has recognized in this context that sharing data "in the spirit of reciprocity for international cooperation" qualifies as an "important public interest" under Article 49.[3] The U.S. government frequently shares intelligence information with EU Member States, including data disclosed by companies in response to FISA 702 orders, based on longstanding cooperative arrangements between the intelligence agencies of the United States and Member States.[4]

---

[2] *Schrems II* judgment § 202 ("[I]n view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under [Article 45] or appropriate safeguards under [Article 46].").

[3] EDPB, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* at 2.4 (25 May 2018) ("the derogation only applies when it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation."). While the EDPB's post-*Schrems II* guidance recognizes that "public interest" transfers need not be "occasional," it cautions that they should not become "the rule." EDPB, *Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18* at 4 (23 July 2020). *See also* EDPB, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* at 4 ("derogations must be interpreted restrictively" and should not be used for "systematic and repeated" transfers).

[4] The United States has long maintained strong partnerships with Europe to respond jointly to shared threats. In 2019, then-Director of National Intelligence Daniel Coats testified before the Senate Select Committee on Intelligence that the United States works closely with EU Member States, through our NATO alliances, to address threats from foreign states, like Russia, who seek to sow divisions between like-minded democracies. Testimony of Director of National Intelligence Daniel Coats

This information is critical to our collective security and is routinely shared with Member State and other governments to counter a variety of threats, including international terrorism, the proliferation of weapons of mass destruction, and the activities of hostile foreign cyber actors. In 2014 the U.S. Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent oversight entity, conducted an extensive review of FISA 702, including assessing its efficacy. After reviewing fifty-four cases in which FISA 702 information was used in intelligence matters, the PCLOB found that "approximately forty cases *exclusively* involved operatives and plots in foreign countries."[5]

As an example of such a case, on December 31, 2016 a gunman killed 39 people and injured 69 others at a Turkish nightclub before fleeing the scene. Public reporting indicates the wounded and dead included EU citizens from France, Germany, and Bulgaria. Almost immediately, Turkish law enforcement and U.S. intelligence officials began cooperating to identify and locate the shooter. Part of that effort included intelligence collection under FISA 702. The information derived from FISA 702 collection ultimately led police to an apartment in Istanbul where an Uzbek national was arrested, and firearms, ammunition, drones, and over $200,000 in cash were seized.[6] This individual was tried and convicted, and in September 2020 was sentenced to life imprisonment.

Because of the need to protect national security information, the U.S. government cannot disclose most of the instances in which the FISA 702 program has protected the safety of EU citizens and residents. However, the following declassified examples demonstrate the types of benefits that accrue to EU citizens from this program:[7]

- The National Security Agency ("NSA") produced a body of reporting based on FISA 702 collection highlighting the 2015 travel of several extremists from the Middle East to Europe, likely for the purpose of conducting terror attacks. One of these travelers was directed by, and maintained contact with, one of the planners of the 2015 Paris attacks, reporting the problems

---

before the U.S. Senate Select Committee on Intelligence (29 Jan. 2019), available at link. Similarly, in 2015, then-Secretary of Defense Ashton Carter and the French Minister of Defense Mr. Jean-Yves Le Drain, issued a joint statement that spoke at length about our alliance, to include sharing of intelligence, available at link.

[5] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" at 109-110 (2 July 2014) (emphasis added) ("PCLOB FISA 702 Report"), available at link.

[6] *See* ODNI, "Guide to Section 702 Value Examples" at 4-5 (Oct. 2017), available at link.

[7] *See* NSA, "'Section 702' Saves Lives, Protects the Nation and Allies" (12 Dec. 2017), available at link.

and difficulties he encountered throughout his journeys. NSA provided identifying information to foreign partners, who located and detained the individual for criminal prosecution.

- In late September 2015, NSA received information from a partner nation about the activities of an extremist, who aspired either to travel to the Middle East to join an extremist group, or to conduct a terrorist attack on European soil. Based on that tip, NSA used FISA 702 collection to acquire the extremist's communications, which allowed the agency to tip the partner nation to the individual's plans to carry out an attack on a public area. This timely foreign intelligence information assisted partner nation authorities with pinpointing the extremist's location and activities. NSA was credited by the partner nation with providing key information for the investigation, which resulted in the extremist's overseas arrest.

- NSA reporting based on FISA 702 collection helped thwart the efforts of front companies seeking to obtain weapons probably bound for a rebel group in the Middle East. Information derived from FISA 702 was shared with a European government, which prompted that government to prevent a nearly $1 million shipment of weapons and ammunition. This European government also revoked the export license of multiple arms companies based on the intelligence.

- NSA analysis of FISA 702 collection discovered the communications of a member of a major terrorist group in the Middle East who was communicating with an extremist in Europe who was sharing ideas on how to commit a terrorist attack. NSA discovered communications where the two individuals discussed buying material to build a suicide belt. NSA shared this information with European partners in an attempt to disrupt further attacks against U.S. and allied interests.

In 2014 the PCLOB reported that "[o]ver a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on section 702 collection, and this percentage has increased every year since the statute was enacted."[8] Sharing of FISA 702 information undoubtedly serves important EU public interests by protecting the governments and people of the Member States. Likewise, the interruption of FISA 702 collection would severely and adversely impact EU public interests.

[8] PCLOB FISA 702 Report at 108.

Companies Relying on Standard Contract Clauses

As noted above, companies transferring personal data from the EU to the United States may choose to rely on SCCs, which the ECJ expressly upheld in *Schrems II* with the caveat that companies are responsible for determining whether the law of the United States ensures adequate protection as afforded in EU law, including by providing, where necessary, additional safeguards.[9] For companies making that determination, the remainder of this White Paper identifies information about relevant U.S. law and practice.[10]

It is important to note that *Schrems II* was *not* a ruling on whether privacy protections in U.S. law *per se*, as of either 2016 or 2020, are consistent with EU law. The ECJ ruled only on the validity of Decision 2016/1250,[11] and the ECJ's assessment of U.S. law accordingly relied primarily on the limited findings about U.S law recorded by the Commission in 2016 in Decision 2016/1250.[12] By contrast, companies using SCCs today to transfer data to the United States may consider all currently available information about U.S. law, including (1) information not recorded in Decision 2016/1250; and (2) new developments that have occurred since 2016. Below, we identify relevant information for the two sources of U.S. intelligence law for which the ECJ reviewed the Commission's findings in Decision 2016/1250: FISA 702 and EO 12333, with a particular focus on those issues that appear to have concerned the ECJ in *Schrems II*.

FISA 702

The Supervisory Role of the FISC over Individual Targeting Decisions

One concern the ECJ raised in *Schrems II* with FISA 702 is whether the Foreign Intelligence Surveillance Court ("FISC")—the federal court staffed by independent, life-tenured judges whom the FISA statute authorizes to approve and oversee foreign intelligence surveillance—supervises whether individuals are

[9] *Schrems II* judgment § 134.

[10] Companies using other bases for transfer requiring appropriate safeguards, such as Binding Corporate Rules under GDPR article 47, may likewise consider the information in this White Paper.

[11] *Schrems II* judgment § 161 ("it should therefore be examined whether the Privacy Shield Decision complies with the requirements [of EU law]"); *id.* §§ 201, 203(5) (ruling Decision 2016/1250 invalid).

[12] *Id.* §§ 179-183, 190-196 (citing Decision 2016/1250 at least ten times in reviewing U.S. law).

properly targeted.[13] A review of applicable U.S. law and practice demonstrates that the FISC is in fact actively involved in supervising whether individuals are properly targeted under FISA 702.

By way of background, before the U.S. government may acquire under FISA 702 the communications data of any person (including an EU citizen or resident) meeting certain targeting restrictions, the FISC must—absent exigent circumstances—approve a written certification submitted by the Attorney General and the Director of National Intelligence jointly authorizing the collection activities for up to one year.[14] Among other requirements, the certification must be accompanied by and the FISC must approve targeting procedures defining how the government determines which specific persons' communications may be acquired.[15] The certification also limits the purpose of the surveillance to a specified type of foreign intelligence—for example terrorism or the acquisition of weapons of mass destruction.[16]

The targeting procedures approved by the FISC are binding on the government[17] and specify how a "selector"—an account identifier such as an email address or telephone number of an individual—may be "tasked" to acquire the type of foreign intelligence specified in the certification.[18] If the FISC approves the certification, the government may issue "directives" to electronic communication service providers in the United States.[19] These directives compel the providers to disclose communications data of specific persons in response to targeted requests based on the tasked selectors.[20]

---

[13] *Id.* §§ 179-80.

[14] 50 U.S.C. §§ 1881a(a),(g) (2018).

[15] *Id.* § 1881a(h).

[16] PCLOB FISA 702 Report at 6.

[17] Failure to adhere to the court-approved targeting procedures must be reported to the FISC as an incident of non-compliance under the terms of the FISC Rules of Procedure, dated 1 November 2010, available at link. Rule 13(b) states that "the government, in writing, must immediately inform the Judge to whom the submission was made of … the non-compliance … and … how the government proposes to dispose of or treat any information obtained as a result of the non-compliance."

[18] *See, e.g.*, NSA Section 702 Targeting Procedures (23 Mar. 2018), available at link. *See also* PCLOB FISA 702 Report at 41-47.

[19] 50 U.S.C. § 1881a(i) (2018).

[20] *Id.* Selectors cannot consist of general key words such as "bomb" or "attack," or even the names of individuals, because such terms would not identify specific communications accounts. *See* PCLOB FISA 702 Report at 33. Even before more

The Commission in Decision 2016/1250 did not record how the FISC supervises and enforces compliance with these targeting requirements.[21] The government must record in every case the reasons a specific person was targeted. The FISA 702 targeting procedures approved annually by the FISC have long required intelligence analysts to "determine that tasking the selector will be likely to acquire one of the types of foreign intelligence information identified in a Section 702 certification" approved by the FISC.[22] The targeting procedures also now require that when making this assessment, analysts at the NSA must "provide a written explanation of the basis of their assessment, at the time of targeting."[23] Requiring NSA analysts to record their "targeting rationale" when tasking selectors facilitates the FISC's supervision of whether individuals are properly targeted by "memorializ[ing] why the analyst is requesting targeting, and provid[ing] a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked."[24] This provides oversight offices a record of the basis for each tasking decision at the time of tasking, which allows for better reporting to the FISC on whether individuals were properly targeted.

Each and every targeting assessment and rationale made by NSA analysts and each and every selector tasked for data acquisition is reviewed by independent intelligence oversight attorneys in the Department of Justice ("DOJ") for compliance with the applicable legal standard set forth in the targeting procedures. The DOJ section performing this function is then responsible for reporting compliance incidents to the FISC. It conducts this oversight function independent from foreign

---

recent changes in U.S. law and practice, the PCLOB expressly found in 2014 that FISA 702 "is not based on the indiscriminate collection of information in bulk." *Id.* at 111.

[21] The Commission tangentially referenced the FISC's supervisory role. Commission Implementing Decision 2016/1250 of 12 July 2016 on the Adequacy of the Protection Provided by the EU-US Privacy Shield, OJ 2016 L 207/1 ("Decision 2016/1250") §§ 109-110 (referring to the government reporting FISA 702 compliance incidents to the FISC, and government plans to provide the FISC certain targeting information, but not discussing the FISC's own active supervisory role over whether individuals are properly targeted to acquire foreign intelligence information).

[22] PCLOB FISA 702 Report at 45.

[23] *E.g.*, NSA Section 702 Targeting Procedures at 8 (Mar. 2018), available at link. This requirement was added to the targeting procedures that were publicly released in 2017 and thus could not have been recorded by the Commission as part of Decision 2016/1250.

[24] Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the FISA, Submitted to the FISC by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. A-6 (October 2018) ("DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017"), available at link.

intelligence priorities, and it has frequent meetings and discussions regarding oversight of FISA 702 targeting with the FISC. The section's lawyers owe a legal duty of candor to the FISC, and under a long-established rule of the court are required to report to the FISC any violations of FISA 702 targeting procedures.[25] Thus in this respect, the FISC supervises the NSA's assessments that individuals have been properly targeted for purposes of acquiring foreign intelligence information.

The FISC can and does enforce compliance with FISA 702 targeting requirements, including by imposing remedial action. Moreover, the FISC has made clear that its review of FISA 702 targeting procedures is not confined to the procedures as written, but also includes how the government implements those procedures.[26] The FISC conducts its own compliance analysis and—in oral hearings or through written responses—can require the government to explain compliance incidents and describe how they have been remedied. If the court is not satisfied, it can terminate the government's authority to engage in data acquisition, including through binding remedial decisions. Most records of the FISC's interactions with the government are classified, but some have been released. For example, documents released pursuant to Freedom of Information Act litigation are posted on a U.S. Intelligence Community website.[27] These and other released documents confirm the FISC's hands-on supervisory role, including by revealing that the FISC has posed detailed questions to the government on how FISA 702 targeting and minimization procedures are implemented.[28] Also publicly available are the government's lengthy reports to the FISC in response.[29] The FISC's scrutiny of the government's

[25] FISC Rules of Procedure (2010), Rule 13(b), available at link. *See* PCLOB FISA 702 Report at 70-75.

[26] *E.g.*, FISC, Memorandum Opinion and Order at 7 (6 Nov. 2015), available at link.

[27] *E.g.*, ODNI, *IC on the Record*, "DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of FISA," available at link.

[28] *E.g.*, Transcript of Hearing before FISC (4 Aug. 2014) at 2-8 (chief of DOJ intelligence oversight section answering questions from FISC about government's implementation of targeting requirements), available at link; FISC, Follow-up Questions Regarding Section 702 Certification (17 June 2011) (listing 16 detailed questions, with sub-questions, about the government's implementation of FISA 702 targeting and minimization procedures), available at link.

[29] *E.g.*, FISC Memorandum Opinion and Order at 4-5 (26 April 2017) (referring to several rounds of government reporting in response to questions from the FISC), available at link; Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications (15 Nov. 2011) (12 pages of responses to FISC's technical questions on procedures compliance), available at link.

submissions concerning the FISA 702 program can lead to modifications, delays, or termination of FISA 702 data collection.[30]

The rigor and effectiveness of the FISC's supervision of whether individuals are properly targeted is demonstrated in semi-annual joint assessments that DOJ and the Office of the Director of National Intelligence ("ODNI") provide to the FISC.[31] As noted above, *each* individual selector tasked for data acquisition is reviewed for compliance with the targeting procedures. DOJ and ODNI conduct onsite reviews at NSA on a bimonthly basis.[32] Prior to each onsite review, NSA electronically sends DOJ and ODNI the tasking record for each selector tasked during the bimonthly review period.[33] In the semi-annual assessments, as well as in more frequent reporting, DOJ and ODNI report each targeting compliance incident to the FISC; identify targeting compliance trends; provide the court with statistical data and describe categories of compliance incidents; and review in detail for the FISC the reasons certain targeting compliance incidents occurred, and the measures intelligence agencies have taken to avoid recurrence.[34]

The public record shows reporting to the FISC of incidents involving whether foreign nationals are properly targeted. For example, a joint DOJ-ODNI oversight assessment submitted to the FISC in late 2016 discusses an NSA targeting office's misapplication of the "foreign intelligence" targeting requirement. The NSA office erroneously tasked a selector when it did not have sufficient information to assess that the user of the selector would communicate the type of foreign intelligence authorized under the applicable FISA 702 certification. The report to the FISC indicates the specific remedial steps that were taken in response to this incident, including additional training and guidance to all NSA personnel involved regarding the requirements of the targeting procedures.[35] The report also informs the FISC that in all such "compliance incidents, any data acquired as a result of such tasking and

[30] *See, e.g.*, FISC Memorandum Opinion and Order at 11-25 (26 April 2017) (reauthorizing FISA 702 program only after the government made changes to address the FISC's concerns, including by terminating "about" collection), available at link.

[31] Redacted version of these semi-annual reports are available at link.

[32] *See, e.g.*, DOJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at 8-11, available at link.

[33] *See, e.g.*, *id.* at 10.

[34] *See, e.g.*, *id.* at 28-47.

[35] Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of FISA, Submitted to the FISC by the Attorney General and the Director of National Intelligence, Reporting Period: June 1, 2015 – November 30, 2015 at 35-36 (Nov. 2016), available at link.

detasking errors—regardless of whether or not the user proves to be a United States person or person in the United States—is required to be purged."[36]

The FISC has stated that"[i]t is apparent to the Court that the implementing agencies, as well as [ODNI] and [DOJ], devote substantial resources to their compliance and oversight responsibilities under Section 702. As a general rule, instances of non-compliance are identified promptly and appropriate remedial actions are taken, to include purging information that was improperly obtained or otherwise subject to destruction requirements under applicable procedures."[37] On a separate occasion, the FISC described the government's oversight of FISA 702 targeting as "robust."[38]

In sum, while the ECJ when invalidating Decision 2016/1250 appears to have concluded that the FISC lacked a supervisory role over whether individuals are properly targeted under FISA 702 because the FISC's *ex ante* approvals are programmatic,[39] there is significant information demonstrating that the FISC *does* have an active role in supervising whether individuals are properly targeted to acquire foreign intelligence information. Some of this information was not recorded by the Commission in 2016 or reflects developments since 2016, and other information was not addressed by the ECJ. All of this information may be considered by companies relying on SCCs for data transfers. Again, the key publicly available documents and legal resources that demonstrate that the FISC is actively engaged in supervising individual targeting decisions under FISA 702 include:

1. Decisions, Orders, and Memorandum Opinions of the FISC discussing its supervisory role over the propriety of individual targeting under FISA 702, including those available at link, link, and link.

[36] *Id.* at 43.

[37] FISC, Memorandum Opinion and Order (2014), available at link.

[38] FISC, Memorandum Opinion and Order n. 36 (6 Nov. 2015) (referring to the government providing the FISC "extensive briefing on its oversight activities" including a review of sample tasking sheets, which together "confirmed the Court's earlier understanding that the government's oversight efforts with respect to Section 702 collection are robust."), available at link.

[39] The ECJ found that "the supervisory role of the FISC . . . does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information.'" *Schrems II* judgment §§ 179-80. The ECJ made that finding, however, not based on any discussion in Decision 2016/1250 relating to the FISC's supervision of whether individuals are properly targeted under FISA 702. Instead, the ECJ appeared to rely on a quotation from Decision 2016/1250 stating that the FISC does not authorize individual surveillance measures, but only authorizes FISA 702 surveillance programs. *Id.* § 179. Consistent with the ECJ's decision, companies may consider additional information as described above in undertaking their own independent reviews of U.S. law for purposes of SCC transfers.

2. National Security Agency FISA 702 Targeting Procedures, for 2017, 2018, and 2019.

3. Records of questions posed by the FISC to the government about compliance with FISC-approved procedures, and government responses to the FISC, including those available at link.

4. Semi-annual joint assessments on FISA 702 oversight provided to the FISC by the Attorney General and the Director of National Intelligence, available at link.

Individual Redress for Violations of FISA 702

In *Schrems II*, the ECJ voiced a second concern with FISA 702, namely, whether U.S. law provides individual redress for violations of the FISA 702 program.[40] A review of applicable U.S. law demonstrates that several U.S. statutes authorize individuals of any nationality (including EU citizens) to seek redress in U.S. courts through civil lawsuits for violations of FISA, including violations of Section 702. This information was not addressed by the ECJ in *Schrems II*.

For example, the FISA statute itself empowers a person who has been subject to FISA surveillance and whose communications are used or disclosed unlawfully to seek compensatory damages, punitive damages, and attorney's fees against the individual who committed the violation.[41] The Electronic Communications Privacy Act provides a separate cause of action for compensatory damages and attorney's fees against the government for willful violations of various FISA provisions.[42] Individuals may also challenge unlawful government access to personal data, including under FISA, through civil actions under the Administrative Procedure Act ("APA"), which allows persons "suffering legal wrong because of" certain government conduct to seek a court order enjoining that conduct.[43]

In fact, based on lawsuits brought under these statutes, U.S. courts have reviewed the legality of certain government data collection under FISA. In 2015, for example, a federal appellate court ruled in a lawsuit brought under the APA that the government's bulk collection of telephony metadata was not authorized by Section 501 of FISA.[44] The U.S. Congress, with the executive branch's approval, subsequently

[40] *Schrems II* judgment §§ 181, 192.

[41] 50 U.S.C. § 1810 (2018).

[42] 18 U.S.C. § 2712 (2018).

[43] 5 U.S.C. § 702 (2018).

[44] *See ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). It should be noted that other courts hearing challenges to the same intelligence program reached different results. *See Klayman v. Obama*, 957 F. Supp. 2d 1, 19-25 (D.D.C. 2013) (finding that

terminated that program. Notably, in a development that occurred after the Commission issued Decision 2016/1250 in 2016, a plaintiff persuaded a federal appellate court that it could, at least as a facial matter, seek redress under the APA based on a challenge to the legality of surveillance under FISA 702. That litigation remains pending.[45]

Thus while the ECJ when invalidating Decision 2016/1250 found certain other legal instruments provided no means of individual redress for violations of FISA 702,[46] companies may consider the above information about relevant U.S. statutes not addressed by the ECJ in making their own determinations regarding SCC transfers. To reiterate, the following statutes establish means of individual redress for violations of FISA 702:

1. Section 1810 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810 (2018).

2. Section 2712 of the Electronic Communications Privacy Act, 18 U.S.C. § 2712 (2018).

3. Section 702 of the Administrative Procedure Act, 5 U.S.C. § 702 (2018).

---

plaintiffs could not bring suit under the APA alleging violations of the FISA statute, but could bring suit alleging violations of the Fourth Amendment), *preliminary injunction vacated*, 800 F.3d 559 (D.C. Cir. 2015); *In re Application of the FBI*, No. BR 13-109, 2013 WL 5741573, at *3-9 (FISA Court 29 Aug. 2013) (holding, in *ex parte* proceeding, that the challenged bulk telephony collection program was consistent with the FISA statute).

[45] *Wikimedia Foundation v. National Security Agency* (4th Cir. 2017) (reversing district court holding that Wikimedia had failed to establish standing, as a facial matter, to challenge "Upstream" collection under FISA Section 702, and remanding to district court to determine the government's factual challenge to Wikimedia's standing). Late last year, the government prevailed in the district court on its factual challenge, a decision that the plaintiffs have appealed. *Wikimedia Foundation v. National Security Agency*, 427 F. Supp. 3d 582 (2019), *appeal docketed*, No. 20-1191 (4th Cir. Feb. 21, 2020). To be sure, the U.S. government maintains its position in some cases that certain plaintiffs may lack standing (and therefore lack a cause of action) as a matter of law, just as claimants in EU Member States' courts lack standing if they cannot show they are directly affected by alleged legal violations. *See, e.g.*, EU Fundamental Rights Agency, Intelligence Report Volume I at 67 ("EU FRA Intel. Rep't Vol. I") (German court in 2014 ruling inadmissible a claim of unlawful surveillance that did not show the claimant had been personally affected by the alleged surveillance activity), available at link.

[46] The ECJ, relying on Decision 2016/1250, found that neither of two specified presidential directives governing FISA 702—Executive Order 12333 and Presidential Policy Directive 28—grants individuals actionable rights before U.S. courts. *Schrems II* judgment §§ 181, 192. Consistent with the ECJ's decision, companies may consider the information set out above in undertaking their own independent reviews of U.S. law for purposes of SCC transfers. The Commission referred to the three statutes discussed above in Decision 2016/1250, at §§ 112-13, but the ECJ did not make any findings related to those statutes in setting forth its reasons for invalidating Decision 2016/1250.

FISA 702 Privacy Safeguards Added Since 2017

Numerous additional privacy safeguards have been added to FISA 702 since Decision 2016/1250 was issued in July 2016. We discuss two examples here.

On April 26, 2017 the FISC issued an order terminating the legal authority to conduct acquisition of so-called "about" collection under FISA 702.[47] "About" collection was a form of FISA 702 collection that acquired communications not to or from a tasked selector, but which contained the selector in the text of the communication.[48] The government's termination of "about" collection was accompanied by new NSA targeting procedures implementing the change, stating that "[a]cquisition conducted under these procedures will be limited to communications to or from persons targeted in accordance with these procedures."[49] The elimination of "about" collection reduces the potential for collection of personal data of EU (and other non-U.S.) citizens because their communications now may no longer be acquired under FISA 702 solely because a communication contains a reference to a lawfully tasked selector.

Separately, in early 2018, the U.S. Congress passed, and the President signed into law, additional privacy protections and safeguards relating to FISA 702 through amendments to FISA and other statutes. These amendments included (1) requiring that with each annual FISA 702 certification, the government must submit and the FISC must approve querying procedures, in addition to targeting procedures and minimization procedures; (2) requiring additional steps including notification to Congress before the government may resume acquisition of "about" collection under FISA 702; (3) amending the enabling statute for the PCLOB to allow it to better exercise its advisory and oversight functions; (4) adding the Federal Bureau of Investigation and NSA to the list of agencies required to maintain their own Privacy and Civil Liberties Officers, instead of being subject only to their parent department-level officers, to advise their agencies on privacy issues and ensure there are adequate procedures to receive, investigate, and redress complaints from individuals who allege that the agency violated their privacy or civil liberties; (5) extending whistleblower protections to contract employees at intelligence agencies; and (6) imposing several additional disclosure and reporting requirements on the government, including to provide annual good faith estimates of the number of FISA 702 targets.[50]

[47] FISC Memorandum Opinion and Order at 25 (26 Apr. 2017).

[48] PCLOB FISA 702 Report at 7, 36-39.

[49] NSA Section 702 Targeting Procedures pt. I (29 Mar. 2017), available at link.

[50] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (19 Jan. 2018).

The ECJ's basis in *Schrems II* for invalidating Decision 2016/1250 obviously could not have taken into account these additional FISA 702 privacy safeguards, which were introduced after Decision 2016/1250 was issued. Companies, however, may take into consideration these additional FISA 702 privacy safeguards in their own independent reviews of current U.S. law for purposes of SCC transfers. The following documents relevant to these FISA 702 privacy safeguards, in addition to information about other privacy safeguards not addressed by the ECJ, may be found on "IC on the Record," the website that ODNI maintains on behalf of the U.S. Intelligence Community:[51]

1. FISC order of 26 April 2017, available at link.

2. NSA Section 702 Targeting Procedures (29 Mar. 2017), available at link.

3. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (19 Jan. 2018).

"Essential Equivalence"

Finally, as to the question whether privacy protections in FISA 702 meet EU legal standards by providing protections "essential equivalent" to protections afforded in the EU,[52] the FISC's role in authorizing and supervising FISA 702 targeting decisions compares favorably with intelligence programs in the EU. The EU itself has no competence over national security matters, which are the sole responsibility of the EU Member States. Only about half of the Member States as of 2015 required *any* form of judicial review for intelligence collection of personal data.[53] The European Court of Human Rights ("ECtHR") regularly reviews the domestic intelligence surveillance programs of Member States and has upheld programs that are similar to or more expansive than FISA 702.[54] Several Member States' domestic intelligence

[51] ODNI, *IC on the Record*, https://icontherecord.tumblr.com/.

[52] *See Schrems II* judgment § 96 (privacy safeguards for SCC data transfers must ensure "a level of protection essentially equivalent to that which is guaranteed within the European Union.").

[53] EU FRA Intel. Rep't Vol. I at 51-52 ("just over half [of Member States] charge the judiciary (judges or prosecutors) with the [surveillance] approval process, while others charge ministers, prime ministers, and expert bodies"), available at link.

[54] *See, e.g.*, *Centrum För Rättvisa v. the Kingdom of Sweden*, No. 35252/08 ECtHR §§ 18-20 (19 June 2018), referred to the Grand Chamber on 4 February 2019 and in which a hearing took place in July 2019 (upholding Sweden's interception of international communications through use of categories of search terms, where approved by its Foreign Intelligence Court and subject to later supervision by Swedish oversight authorities); *Weber and Saravia v. Germany*, No. 54934/00 §§ 4, 97, 117 (29 June 2006) (upholding Germany's "strategic monitoring" involving interception of international communications through use of "catchwords capable of triggering an investigation into" listed national security dangers, where authorized and subject to oversight by an independent commission).

programs go beyond targeted surveillance to include bulk collection—the EU's Fundamental Rights Agency found in 2015 that among five Member States with laws regulating untargeted intelligence collection, three allowed for untargeted surveillance domestically, while others appeared not to substantially regulate their surveillance of communications at all.[55] The reality is that data transferred to the United States enjoys comparable or greater privacy protections relating to intelligence surveillance than data held within the EU.[56]

Executive Order 12333

EO 12333 is a general organizing directive that (1) assigns the different U.S. intelligence agencies responsibility for different types of overt and clandestine intelligence collection and counterintelligence activities, and (2) places restrictions on certain agencies' activities.[57] Unlike FISA 702, however, EO 12333 does not authorize the U.S. government to *require* any company or person to disclose data. Any requirement that a company in the United States disclose data to the government for intelligence purposes must be authorized by statute and must be targeted at specific persons or identifiers, such as through FISA 702 orders as discussed above; bulk collection is expressly prohibited.[58] Of course, a

[55] *See* EU Fundamental Rights Agency, *Report on Surveillance by intelligence services, Volume II: field perspectives and legal update* at 42-43 (2017) ("EU FRA Intel. Rep't Vol. II") (discussing laws of France, Germany, the Netherlands, Sweden, and the United Kingdom), available at link. The FRA's survey of those five Member States is itself "in no way exhaustive," as other Member States "might allow for general surveillance of communications – but they do not regulate it in detail." *Id.* at 42. *See also* Bulk Collection: Systematic Government Access to Private-Sector Data (eds. Fred H. Cate & James X. Dempsey, 2017) at xxviii ("[T]he only country that has conclusively terminated a bulk collection program in recent years is the United States"; "[m]eanwhile, the UK, France, Germany and other countries have ratified or expanded collection programs").

[56] For a broader comparative discussion of U.S. and Member State law and practice establishing privacy protections related to intelligence agencies' access to personal data, see the Written Legal Submission on Behalf of the United States of America as Amicus Curiae, in *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems* (23 Dec. 2016) (High Court) (Ireland), available at link.

[57] For example, EO 12333 authorizes the Central Intelligence Agency to collect foreign intelligence including through clandestine means and conduct counterintelligence activities, but prohibits the agency from performing internal security functions or engaging in electronic surveillance (with limited exceptions) within the United States. EO 12333 §§ 1.7(a)(1)-(2), 2.4(a).

[58] Under U.S. law, any government demand that a company in the United States receiving data from the EU under SCCs disclose the data for intelligence purposes must be authorized either by FISA or the National Security Letter ("NSL") statutes. In addition to Section 702, FISA authorizes five other types of data collection potentially involving such transfers. 50 U.S.C. § 1801 *et seq*. (electronic surveillance of persons located in the U.S.), § 1821 *et seq*. (physical searches), § 1841 *et seq*. (communication transactional data and subscriber information), § 1861 (business records), § 1881b (acquisition in the U.S. of data about a U.S. person located abroad). The NSL statutes authorize government demands for certain financial and communications records (not including the content of communications) from third-party companies in the United States. 12

company may always choose whether to cooperate voluntarily with an intelligence agency's data collection efforts where not prohibited by law.

As companies relying on SCCs make determinations about privacy protections in U.S. law, it is unclear how they would consider any U.S. national security data access other than targeted government requirements for disclosure such as under FISA 702. By comparison, when the ECJ evaluated Decision 2016/1250 in *Schrems II*, it began its review of data access under EO 12333 and FISA 702 by citing the applicable derogation permitting U.S. companies participating in Privacy Shield to disclose data "to the extent necessary to meet [U.S.] national security [and other government] requirements."[59] But under EO 12333, there can be no "requirement" for a company to disclose any data to the U.S. government. And the government certainly may not legally require U.S. companies to disclose data transferred under SCCs "in bulk," which was the aspect of EO 12333 collection about which the ECJ expressed concern in *Schrems II*.[60] Bulk data collection is permitted only in other contexts, such as clandestine intelligence activities involving overseas access to data—activities in which companies cannot legally be compelled to participate.

Regarding the possibility of the U.S. government unilaterally obtaining access overseas under EO 12333 to data being transferred from the EU, it is unclear how companies using SCCs could assess whether U.S. privacy protections relating to such hypothetical access meet EU legal standards, for several reasons. First, during transfer from the EU to the United States, data is potentially subject to unilateral access by many actors. Many countries around the world, including the United States and EU Member States, collect information for intelligence purposes outside of their territories. Data transferred outside the EU, whether destined for the United States or any other country, flows through numerous transmission networks and is potentially subject to access by such countries' intelligence agencies, as well as by private entities acting illicitly, and will be more or less protected from such access depending on the data security measures taken by a company and on the laws and practices in each jurisdiction through which the data passes. No country acknowledges the specific locations and operational details of its clandestine overseas intelligence activities. Many countries do not even regulate such activities by law, including some EU Member States.[61] Were the lawfulness of data transfers outside the EU to depend on an

---

U.S.C. § 3414; 15 U.S.C. §§ 1681u and v; 18 U.S.C. § 2709; and 50 U.S.C. § 3162. Both the FISA and NSL statutes prohibit collection of data in bulk.

[59] *Schrems II* judgment §§ 164-65.

[60] *Id.* § 183.

[61] *See* EU FRA Intel. Rep't Vol. II at 42 (2017) (some Member States "might allow for general surveillance of communications–but they do not regulate it in detail"), available at link.

assessment of intelligence agencies' clandestine access to data outside a given destination country while in transit, no data transfers could be found lawful under EU standards because intelligence agencies worldwide potentially could access the data as it travels over global networks.

A second reason companies using SCCs may not be able to assess whether U.S. privacy protections relating to hypothetical overseas government access to data under EO 12333 meet EU legal standards is that there is no discernable comparator in EU law. The ECJ has never ruled on the lawfulness of a Member State's overseas access to data for intelligence purposes, and it may not have jurisdiction to do so given restrictions in the EU treaties.[62] And while the ECtHR has for decades reviewed EU Member States' intelligence surveillance programs, those cases have involved only domestic surveillance programs—that is, government access to communications or other data *within* a state's territorial jurisdiction. This is true, for example, for all the ECtHR decisions cited in the *Schrems II* Advocate General's assessment of Decision 2016/1250.[63] Indeed, in each of the three of those decisions not actually brought by residents of the respondent state, the ECtHR made clear that its review concerned only domestic surveillance *within* the respondent state's territorial jurisdiction.[64]

---

[62] *E.g.*, Treaty on European Union art. 4(2) ("The Union shall respect [the Member States'] essential State functions . . . . In particular, national security remains the sole responsibility of each Member State.").

[63] *Big Brother Watch and Others v. United Kingdom*, Nos. 58170/13, 62322/14 & 24960/15 §§ 56-95 (13 Sept. 2018) (sixteen persons and organizations from different countries challenging the United Kingdom's Regulation of Investigatory Powers Act authorizing the interception of communications subject to the United Kingdom's territorial jurisdiction); *Ben Faiza v. France*, No. 31446/12 (8 Feb. 2018) (resident of France challenging France's Code of Criminal Procedure authorizing fixing of geolocation device onto vehicle and disclosure of telephone records); *Szabó and Vissy v. Hungary*, No. 37138/14 §§ 6-17 (12 Jan. 2016) (residents of Hungary challenging Hungary's Police Act authorizing intelligence surveillance measures); *Zakharov v. Russia*, No. 47143/06 ECtHR §§ 25-138 (4 Dec. 2015) (resident of Russia challenging Russia's Operational-Search Activities Act authorizing interception of telephone communications, and regulations issued thereunder); *Kennedy v. United Kingdom*, No. 26839/05 ECtHR §§ 25-74 (18 May 2010) (resident of United Kingdom challenging United Kingdom's Regulation of Investigatory Powers Act authorizing interferences with telecommunications); *Liberty and Others v. United Kingdom*, 58243/00 §§ 5, 15-17 (1 July 2008) (civil liberties organizations from United Kingdom and Ireland challenging the United Kingdom's Interception of Communications Act authorizing interception of communications at facility in United Kingdom); *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 62540/00 §§ 6-28 (28 June 2007) (non-profit association resident and with registered office in Bulgaria challenging Bulgaria's Special Surveillance Means Act authorizing surveillance through use of technical devices); *Weber and Saravia v. Germany*, No. 54934/00 §§ 3, 14-31 (29 June 2006) (residents of Uruguay challenging "strategic monitoring" under Germany's "G 10 Act" authorizing the interception of international wireless communications from interception sites on German soil); *Malone v. United Kingdom*, No. 8691/79 §§ 12, 19-30, 63 (2 Aug. 1984) (resident of United Kingdom challenging legal and administrative framework authorizing interception of communications by police in criminal investigation); *Klass and Others v. Germany*, N. 5029/71 ECtHR §§ 10-25 (6 Sept. 1978) (residents of Germany challenging Germany's "G 10 Act" authorizing interferences with mail, post and telecommunications).

[64] *Big Brother Watch and Others* § 271 ("nor did [the applicants] suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom's territorial jurisdiction. The Court will therefore proceed

Furthermore, even if a company using SCCs could determine what is required under EU law, there are privacy safeguards applicable to EO 12333 surveillance in current U.S. law and practice left unaddressed by the ECJ in *Schrems II* that equal or exceed protections afforded in the EU. Notable among these safeguards is Presidential Policy Directive 28 ("PPD-28"), a presidential directive in effect since 2014 that sets binding requirements for signals intelligence activities that afford fundamental privacy safeguards for all people, regardless of nationality or location. For example, PPD-28 delimits the use of signals intelligence collected in bulk to detecting and countering six types of threats: (1) espionage and other threats from foreign powers; (2) terrorism; (3) threats from weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied forces; and (6) transnational criminal threats.[65] PPD-28 also requires each intelligence agency to adopt procedures allowing the retention or dissemination of personal information, regardless of nationality, only if retention or dissemination of "comparable information concerning U.S. persons would be permitted."[66]

In addition, the National Intelligence Priorities Framework ("NIPF") sets out separate criteria to ensure that data acquisition responds to national intelligence priorities. Based on authority derived from statute and from EO 12333,[67] the Director of National Intelligence established the NIPF under Intelligence Community Directive 204, which "promulgates policy and establishes responsibilities for setting national intelligence priorities and translating them into action."[68] The robust process the NIPF has created within the Executive Branch applies objective criteria to ensure that targeting and collection, including bulk signals intelligence under EO 12333, are responsive to specific national intelligence

---

on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom"); *Liberty and Others* §§ 42, 47 (applicants and United Kingdom both proceeding on basis that claimed interception of communications occurred at facility in England); *Weber and Saravia* §§ 86-88 (rejecting claim by the Uruguayan applicants that the surveillance involved extraterritorial measures, noting that "[s]ignals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In light of this, the Court finds that the applicants failed to provide proof . . . that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.").

[65] PPD-28 § 2, available at link. This limitation is referenced at Decision 2016/1250 § 74.

[66] PPD-28 § 4(a)(i), available at link. U.S. intelligence agencies' procedures implementing PPD-28 are publicly available at the following link. This limitation is referenced at Decision 2016/1250 § 74.

[67] National Security Act, 50 U.S.C. § 3024(f)(1)(A)(i)-(ii); EO 12333 § 1.3(b)(17).

[68] ODNI, Intelligence Community Directive 204, *National Intelligence Priorities Framework* § B.1 (2 Jan. 2015), available at link.

priorities. The National Signals Intelligence Committee then translates those priorities into more precise signals intelligence requirements. The committee reviews agency requests for collection, ensures that they are consistent with the NIPF, and assigns them priorities. These priorities are assigned using a range of criteria, including the level of priority reflected in the NIPF; cost-effectiveness; whether collection would be as tailored as feasible; the sensitivity of the target or the methodology; the risk to privacy and civil liberties, regardless of the nationality of the targets; and the need to apply additional dissemination or retention safeguards to protect privacy or national security interests.[69]

Intelligence agencies are also required to have internal procedures governing EO 12333 collection that set out requirements for intelligence officers whenever practicable to identify specific selection terms, such as telephone numbers or email addresses, that are expected to collect foreign intelligence responsive to NIPF priorities. NSA's PPD-28 procedures, for example, highlight privacy concerns raised by the potential acquisition of foreign nationals' personal data, and require the use of selectors.[70] Section 4.1 of those procedures states that "SIGINT activities that take place in response to foreign intelligence requirements . . . may result in the acquisition of communications that contain personal information of non-U.S. persons." Section 4.2 then requires that "[w]henever practicable, collection will occur through the use of one or more SELECTION TERMS in order to focus the collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (e.g., the proliferation of weapons of mass destruction by a foreign power or its agents)." Separately, the Central Intelligence Agency's guidelines issued in 2017—and thus after the Commission issued Decision 2016/1250—require senior approvals and documentation of privacy protections for any bulk data collection.[71]

These and other restrictions on acquisition of personal data (including the data of EU citizens) under EO 12333 are mandatory requirements for the intelligence agencies and enforced in practice through oversight mechanisms, including investigations undertaken by the Inspector General at each intelligence agency. While their reports of investigations regarding intelligence activities are usually classified and thus maintained as secret within the government, Inspectors General sometimes report publicly about

[69] *See* Letter from Robert Litt, General Counsel of the ODNI, annexed to Privacy Shield framework at 5 (22 Feb. 2016), available at link.

[70] NSA PPD-28 Section 4 Procedures (also titled, as indicated on page 4 of the annex, "Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons"), available at link. Certain related constraints are discussed at Decision 2016/1250 §§ 71-73, 76.

[71] Central Intelligence Agency, Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333 § 5 (19 Jan. 2017), available at link.

violations and about remedial actions taken. In 2013, for example, the NSA Inspector General reported to the Congress that, in the prior decade, there had been twelve substantiated instances of intentional misuse of the NSA's signals intelligence authorities, including unauthorized queries and taskings against foreign nationals.[72] The letter setting out this information identified the enforcement actions (e.g., termination and other disciplinary action) that the NSA had taken against the relevant employees. In addition to enforcement action, agencies like NSA routinely take additional remedial measures—like deleting unauthorized collection—to address individual compliance incidents.[73]

Accordingly, while the ECJ found problematic the lack of precision on the permissible scope of bulk collection under EO 12333,[74] even if a company could find a meaningful basis on which to compare U.S. data protections with protections afforded in the EU, there is significant publicly available information about U.S. privacy protections *not* addressed by the ECJ that companies may wish to consider when undertaking an independent review of U.S. law for purposes of SCC transfers. This includes important information identifying the circumstances under which bulk collection is permitted. The relevant documents and legal resources discussed above are listed below. Those documents and other information about U.S. privacy protections relating to EO 12333 collection may be found on the "IC on the Record" website:[75]

1. Presidential Policy Directive 28 (PPD-28), available at link.

2. Intelligence Community Directive 204, *National Intelligence Priorities Framework*, available at link.

[72] NSA Inspector General's Letter to Senator Grassley (11 Sept. 2013), available at link.

[73] *See* NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333 at 14 (2014) ("Data is required to be deleted from NSA systems if it is found to have been acquired without authorization"), available at link.

[74] The issue with EO 12333 that appeared to concern the ECJ, relying on Decision 2016/1250 and associated Privacy Shield documents, was that it "allows for 'bulk' collection" when necessitated by operational circumstances, and that this possibility does not "delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data." *Schrems II* judgment § 183. Consistent with the ECJ's decision, companies may consider the information set out above in undertaking their own independent reviews of U.S. law for purposes of SCC transfers.

[75] ODNI, *IC on the Record*, https://icontherecord.tumblr.com/.

3. NSA Procedures Implementing Section 4 of PPD-28, also titled "Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons"), available at link.

4. Central Intelligence Agency, Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333 (19 Jan. 2017), available at link.

5. NSA Inspector General's Letter to Senator Grassley (11 Sept. 2013) available at link.

6. NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333 (2014), available at link.

Conclusion

This White Paper focuses on the privacy safeguards in current U.S. law relating to intelligence agencies' access to data that are relevant to the issues that appear to have concerned the ECJ in *Schrems II*. There are numerous other privacy safeguards in this area of U.S. law, not discussed by the ECJ in its review of Commission Decision 2016/1250 in *Schrems II*, that ensure that U.S. intelligence agencies' access to data is based on clear and accessible legal rules, proportionate access to data for legitimate purposes, supervision of compliance with those rules through independent and multi-layered oversight, and effective remedies for violations of rights. Thousands of pages of documents about these privacy safeguards, their implementation, and other intelligence-related matters may be found on the internet site "*IC on the Record*."[76] Public access to this information reflects the U.S. intelligence community's strong commitment to openness and transparency.[77]

[76] ODNI, *IC on the Record*, https://icontherecord.tumblr.com/.

[77] *See* ODNI, *Principles of Intelligence Transparency* (2015) (guiding U.S. intelligence agencies on making information about intelligence activities and oversight publicly available in a manner that enhances public understanding while continuing to protect information that, if disclosed, would harm national security), available at link.