***Schrems II* Concerns Regarding U.S. National Security Surveillance Do Not Apply to Most Companies Transferring Personal Data to the U.S. Under Standard Contractual Clauses**

December 23, 2020 (Revised)

Alan Charles Raul
Partner, Sidley Austin LLP
Former Vice Chairman of the Privacy and Civil Liberties Oversight Board
Former Associate Counsel to the President (Ronald Reagan)

The thesis articulated here is that (1) nearly all companies relying on standard contractual clauses for data transfers to the U.S. under the EU General Data Protection Regulation are not electronic communications service providers for purposes of FISA 702 (i.e., only companies in the business of providing communications services would be covered) and (2) data transfers from Europe to the U.S. under SCCs may not be targeted under FISA 702 and EO 12333 because they are (i) quintessential "US person communications" because either the data exporter is a U.S. person or the data importer is a U.S. person, or more likely, both are U.S. persons and (ii) received by a person located in the U.S. Accordingly, the concerns expressed by the EU Court of Justice in Schrems II should not be problematic for nearly all U.S. companies relying on SCCs.

A concise version of this paper, adapted for Lawfare, is available at https://www.lawfareblog.com/why-schrems-ii-might-not-be-problem-eu-us-data-transfers.

In its July 16 opinion in *Schrems II*,[1] the Court of Justice of the European Union invalidated the U.S.-EU "Privacy Shield" framework that authorized the transfer of personal data from the European Economic Area (EEA) to the U.S. The CJEU also imposed onerous new obligations on the use of "standard contractual clauses" (SCCs) as an alternative mechanism for such transfers.

The Court's fundamental rationale for its restriction on data flows to the U.S. involved concerns that national security surveillance conducted by the U.S. under two particular authorities could take place without according European data subjects the privacy rights guaranteed in principle in the EU. The two specific authorities troubling the CJEU were Section 702[2] of the Foreign Intelligence Surveillance Act ("Procedures for targeting certain persons outside the United States other than United States persons") and Executive Order 12333 ("United States intelligence activities")[3].

---

[1] Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, *et al*. (July 16, 2020)(*Schrems II*), *available at* http://curia.europa.eu/juris/document/document.jsf;jsessionid=16156EB22BD78B5B5A0B145C0F1D0EF4?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=17987608.

[2] 50 U.S. Code § 1881a - Procedures for targeting certain persons outside the United States other than United States persons, *available at* https://www.law.cornell.edu/uscode/text/50/1881a.

[3] Executive Order 12333 - United States intelligence activities (Dec. 4, 1981), *available at* https://www.archives.gov/federal-register/codification/executive-order/12333.html.

In a nutshell, the CJEU appeared to believe these surveillance authorities involved possible bulk collection with insufficient predication and overly broad targeting criteria, and did not provide sufficient individual redress rights.[4]

This article explains why the CJEU's articulated concerns are quite simply inapplicable to the overwhelming bulk of data transfers to the U.S. under SCCs, and nearly all U.S. companies should have no difficulty meeting the CJEU's obligation to assess those U.S. surveillance authorities (namely 702 and 12333) would not interfere with their ability to comply with SCCs.

As elaborated below, the reason why is simple: surveillance under these authorities may not target communications of U.S. persons (including American companies!), or persons reasonably believed to be in the U.S. Data transfers pursuant to SCCs between an American company in Europe to its American headquarters in the U.S. are exactly the types of communications the NSA may not target under those authorities.

The thesis of this piece may strike those steeped in this subject as either manifestly wrong or insufficiently nuanced, but please read on to understand that even the latter reaction is not warranted. And, the argument here does not turn on the comparative strength of the U.S. system of robust safeguards, judicial and other independent oversight, and an extensive array of checks balances, but rather, on the actual limiting text of the relevant U.S. surveillance authorities themselves.

It would be reasonable to ask why this dramatically consequential reading of the plain text of Section 702 of FISA and EO 12333 would *mirabile dictu* only now surface to help save the future of SCCs. The answer is likely that transfers of corporate EU data to the U.S. have heretofore been viewed as characteristically EU data rather than as quintessential U.S. person data being communicated by one U.S. person (the data-exporting American company) to another U.S. person (the data-importing American company) that is located in the U.S. Such communications simply cannot be targeted under the authorities called into question by the CJEU.

It would also be reasonable to ask whether this same theory should apply to foreign companies transferring data pursuant to SCCs to persons located in the U.S. The answer is, probably yes, so long as there is a U.S. person or person located in the U.S. that is on the receiving side of the SCC transfer, the same prohibitions on targeting should apply. Where American companies

---

[4] Without relitigating *Schrems II*, it is worth pointing out that the independent Privacy and Civil Liberties Oversight Board (PCLOB) issued an oversight on FISA section 702 report stating:

> Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk…. [T]he Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. …. [T]he Board does not regard Section 702 as a 'bulk' collection program, because it is based entirely on targeting the communications identifiers of specific people….

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014) at 103,111, 113, *available at* https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf (PCLOB Section 702 Report).

(U.S. persons) are on both sides of the SCC transfer, rather than just on the receiving end, the privacy protection against U.S. government surveillance would be at its zenith. EU data protection authorities would undoubtedly find this to be an ironic twist – the more American the more private![5]

Without delving into the granular details of the Privacy Shield or SCCs, suffice it to say that the EU's General Data Protection Regulation[6] prohibits transfers of personal data outside the European Economic Area (EEA) to any country whose legal regime for data privacy has not yet been deemed "adequate" by the EU Commission . . . unless the data exporter implements certain approved mechanisms[7] or invokes certain (relatively) narrow derogations[8] (such as individual consent, "public interest," necessity for contractual performance, etc.).

The Privacy Shield was just such a mechanism approved only for transfers to the U.S., while SCCs were approved for general use to authorize data transfers data to any "non-adequate" country, including the U.S. (but potentially also China or Venezuela, or any another country whose privacy regime has not yet been deemed adequate by the EU, or whose privacy regime really is inadequate).

For reasons that will not be rebutted in detail here,[9] the CJEU (at the serial behest of Maximillian Schrems – an Austrian privacy activist) has, sort of, adjudicated the U.S. not to have an "adequate" legal framework for data privacy. Basically, the highest EU court perceives U.S. intelligence agencies to have the authority to collect excessive data to protect U.S. national

---

[5] Note, however, the thesis here that FISA section 702 and EO 12333 are not proper bases to target SCC communications (which are quintessential U.S. person communications) does not mean they could not be targeted under other authorities (or be subject to incidental collection – *i.e.*, non-targeted). Such U.S. person communications could of course be subject to probable cause, business record and other national security and law enforcement authorities. Bear in mind, though, that when SCC data transfers are targeted, the collection of U.S. person communications is not "incidental"– it is necessary, purposeful and intentional. *Cf. U.S. v. Mohamud*, 843 F.3d 420 (9th Cir. 2016)("incidental" collection may comprise collection that is anticipated, "not accidental" and not just "inadvertent"; quoting PCLOB Section 702 Report at 82). Unlike in *Mohamud*¸ where "the government knew *some* U.S. persons' communications would be swept up during foreign intelligence gathering [and that] does not make such collection … unlawful," slip op. at 41(emphasis added), *all* SCC communications are inevitably U.S. person communications.

[6] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(GDPR), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN.

[7] GDPR Article 46 ("Transfers subject to appropriate safeguards" in the absence of an adequacy decision).

[8] GDPR Article 49 ("Derogations for specific situations" for transfers in the absence of an adequacy decision or appropriate safeguards pursuant to Art. 46).

[9] Detailed substantiation that the U.S. national security laws are more than "adequate" compared to the EU can be found in Sidley's 2016 "Essentially Equivalent" Report ("Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States"), *available at* https://www.sidley.com/-/media/publications/essentially-equivalent---final.pdf; the U.S. Government's *Schrems II* White Paper ("Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II") (Sept. 2020), *available at* https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF; and, "The Need for Clarity After Schrems II" in LawFare (by Bradley A. Brooker, Sujit Raman and James M. Sullivan), *available at* https://www.lawfareblog.com/need-clarity-after-schrems-ii.

security, and also, that such agencies suffer from perceived deficits of independent oversight and judicial redress rights and remedies (particularly for non-U.S. persons).

While President Obama's 2014 President Policy Directive (PPD-28) directed U.S. intelligence agencies to respect the privacy rights of foreign citizens in conducting electronic surveillance, the CJEU dismissed this in *Schrems II* as a mere executive order.[10] The text of PPD-28, however, is compelling with regard to the direction to intelligence agencies to protect foreign privacy rights:

> "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information" and "Departments and agencies shall apply the term 'personal information' in a manner that is consistent for U.S. persons and non-U.S. persons. Accordingly, for the purposes of this directive, the term 'personal information' shall cover the same types of information covered by 'information concerning U.S. persons' under section 2.3 of Executive Order 12333."

And as the Office of the Director of National Intelligence has stated in response to the PCLOB report on PPD-28,[11] the Obama Directive is still fully in effect and implemented by intelligence community (IC) agencies:

> "PPD-28 remains in full force and effect. As a formal presidential directive, it has the force of law within the Executive Branch, and compliance is mandatory. As described further below, the IC has systematically implemented the requirements of PPD-28 to ensure that U.S. signals intelligence (SIGINT) activities continue to include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides. IC elements have prepared and published the policies called for by PPD-28, and have been following those policies in conducting their activities."

---

[10] "Presidential Policy Directive -- Signals Intelligence Activities," the White House (2014), sec. 4, n. 7, and *passim*, *available at* https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. PPD-28 requires all intelligence agencies to implement and comply with procedures designed to protect the privacy interests of non-U.S. persons, and all have done so, and directs PCLOB to oversee and report on such procedures, which it does and has done. *See, e.g.*, "PPD-28 Section 4 Procedures: SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF NON-UNITED STATES PERSONS," NSA (2015)("These Supplemental Procedures implement the privacy and civil liberties protections afforded to non-U.S. persons, by Presidential Policy Directive No. 28 (PPD-28), 'Signals Intelligence Activities,' dated 17 January 2014."), *available at* https://fas.org/irp/nsa/nsa-ppd-28.pdf; "Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities," PCLOB (2018)(noting NSA, CIA, and FBI "apply PPD-28 to communications collected under FISA Section 702."), at 4, *available at* https://documents.pclob.gov/prod/Documents/Projects/99da9b42-5e9f-40fd-8ace-94d1e6a7d06c/PPD-28%20Report%20(for%20FOIA%20Release).pdf. *See also* "The Economic Case for Preserving PPD-28 and Privacy Shield," C. Kerry & A. Raul, Lawfare (2017), *available at* https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield.

[11] *See* "Status of Implementation of PPD-28: Response to the PCLOB's Report," Office of the Director of National Intelligence (2018), at 1, *available at* https://www.dni.gov/files/icotr/Status_of_PPD_28_Implementation_Response_to_PCLOB_Report_10_16_18.pdf.

The CJEU's analysis of relevant U.S. laws and facts in *Schrems II* was not terribly substantial. It suffers from considerable blinders (some might say hypocrisy)(because EU intelligence agencies and citizens benefit directly from U.S. intelligence sharing[12]) and double standards (because EU member state surveillance laws and practices do not necessarily compare favorably to those of the U.S.). But the fact is that however fallible its reasoning, the CJEU's judgment is final. Accordingly, unless companies can satisfy the CJEU's concerns, they will not be allowed to use SCCs to transfer personal data of their customers, employees, business contacts, and other individuals, from Europe to the U.S.[13]

In order to continue using SCCs to transfer personal data to the U.S., *Schrems II* (para. 139) obligates the U.S. entity to "certif[y] that it has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the [SCCs] …. and undertakes to notify the data controller about any change in the national legislation applicable to it which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses…."

The only "national legislation" the CJEU calls into question (para. 178) for interference with fundamental rights guaranteed in the EU is "the interference arising from the surveillance programmes based on Section 702 of the FISA and on E.O. 12333." The CJEU makes very clear in *Schrems II* that the basis for its invalidation of the Privacy Shield, and the constraints it imposed on the use of SCCs, is grounded on the problems it identifies with specifically these two U.S. surveillance authorities:

> "184. It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.

---

[12] *See* "Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program," PCLOB (Nov. 19, 2020)("Many of those programs produce significant benefits for European allies, in addition to unilateral benefits for the United States. For example, U.S. agencies frequently share valuable intelligence produced under Section 702 of the Foreign Intelligence Surveillance Act with their European counterparts….Transatlantic discussions about surveillance and privacy could be improved by greater candor about what each side is doing, and why. Ultimately, Americans and Europeans face the same challenge: protecting our societies in a manner consistent with fundamental values and the rule of law.") at 4, *available at* https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf. *See also Schrems II* White Paper, *supra* n. 9, at 4 & n. 7(providing "declassified examples [that] demonstrate the types of benefits that accrue to EU citizens from this [FISA 702] program").

[13] *See generally* European Data Protection Board - 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II (Nov. 11, 2020)("As a result of the [CJEU] ruling on July 16th, controllers relying on Standard Contractual Clauses (SCCs) are required to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data in the third country, if the law of the third country ensures a level of protection of the personal data transferred that is essentially equivalent to that guaranteed in the European Economic Area (EEA). The CJEU allowed exporters to add measures that are supplementary to the SCCs to ensure effective compliance with that level of protection where the safeguards contained in SCCs are not sufficient."), *available at* https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en.

> "185. In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter."

Based on explicit concerns expressed by the CJEU, U.S. entities relying on SCCs should find it dramatically easier to satisfy their self-assessment obligation under *Schrems II* if either (1) they are not an entities subject to Section 702 – i.e., they are not an "electronic communication service provider" or (2) the data they wish to transfer to a person or entity in the U.S. pursuant to SCCs is "U.S. person" data not subject to lawful targeting under Section 702. For the reasons discussed below, the overwhelming bulk of companies transferring data to the U.S. under SCCs are not electronic communications providers within the meaning of Section 702, and they do not transfer data that may be legally targeted for collection under Section 702.

If the above proposition is correct, then the concerns of the CJEU essentially fall away for any U.S. entities that are not among the relatively small number of Section 702 "electronic communication service providers – i.e., the discrete set of companies in the business of transmitting (or storing) communications for third parties – as opposed to the vast number of companies transferring their own customer, employee or business data from their bases in Europe to their bases in the U.S. The reason for this outcome is, quite simply, that Section 702 can only be applied to communications companies and may not be applied to U.S. person data or to data relating to persons located in the U.S. – such as the entity at the importing end of the SCC transfer in the U.S. And, it is critical, of course, that section 702 expressly defines U.S. corporations to be U.S. persons.

The problem is not solved quite as neatly under EO 12333 because this document is not really an authorization to conduct surveillance, but rather, it is a governance document to guide intelligence agencies on how to carry out surveillance outside the U.S. with respect to non-U.S. persons with respect to whom the U.S. Constitution and laws do not apply. For purposes of the analysis here, however, the key proposition is that EO 12333 does not authorize targeting collection against U.S. persons (and is also subject to protecting foreign privacy interests under PPD-28)[14]. And no U.S. company or other U.S. person – indeed no person at all – would ever receive a warrant, court order, or other compulsory process. That is because EO 12333 simply does not authorize, contemplate, or occur with any compulsory legal process at all. Colloquially speaking, EO 12333 is more about spying outside the jurisdiction of U.S. law than surveillance under U.S. law.

In any event, the same principle that absolves the overwhelming bulk of American companies from worrying about Section 702 for their SCC transfers is also true for EO 12333: U.S. intelligence agencies cannot use EO 12333 to avoid the need for a probable cause-type warrant or order, or other lawful authority, to target the content of communications sent by U.S. persons outside the U.S. to U.S. persons located in the U.S.

[14] *See supra* n. 10.

This means that the CJEU's concerns that Section 702 and EO 12333 involve disproportionate data collection that is not "strictly necessary" and "go[es] beyond what is necessary in a democratic society to safeguard" (para. 141) are simply irrelevant for nearly all U.S. companies that rely on SCCs for their data transfers to the U.S. This is not merely an empirical reality – although that is true too[15] – but is an outcome actually directed by the "national legislation" itself. This is exactly what the CJEU would want to see.

1. The category of communications service providers subject to 702 is discrete and does not include the vast bulk of companies that are not in the communications business.

Under the FISA statute, only "electronic communication service providers" can be compelled to comply with Section 702,[16] and any "provider receiving a directive … may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court."[17]

The definition of electronic communication service provider under section comprises: telecom carriers, ISPs, email providers, cloud services, and "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored."[18] While this definition is conceivably broad enough to cover companies that provide their employees with email functionality,[19] that is not

---

[15] *See* U.S. Government "COMMENTS ON PROPOSED SCC DECISIONS (DECEMBER 10, 2020)," submitted to European Commission in response to proposed SCCs, *available at* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries/F1305841, at 9. The U.S.G. comments state:

> For example, the vast majority of U.S. companies doing business in the EU do not, and have no grounds to believe that they, deal in any data that is of any interest to U.S. intelligence agencies. Given U.S. policy not to gather intelligence for purposes of assisting U.S. companies commercially, companies trading in ordinary 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.
>
> In particular, only a very small number of U.S. companies have ever received orders to disclose data under Section 702 of the Foreign Intelligence Surveillance Act, the form of compulsory process of concern to the Court of Justice in Schrems II. The Commission's direction that data exporters should take into account the specific circumstances of each data transfer shows an awareness and sensitivity to these kinds of facts. Highlighting this implication would alleviate unfounded anxiety in the business communities—both in the United States and in the European Union—over the impact of the Schrems II decision on their enterprises. [emphasis added]

[16] 50 U.S.C. 1881a(i)(1)(A) & (i)(5):

> If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

[17] *Id.* (i)(4).

[18] *Id.* 1881(b)(4). Note that cloud providers are typically considered "remote computing services" (RCS) under the Stored Communications Act, and therefore also under FISA. It should also be noted that where the RCS is providing "processing" services in addition to cloud storage, it is possible that the RCS provider could be considered the intended recipient of the communication, not merely a communications or storage conduit.

[19] Under the Stored Communications Act (SCA), however, a corporate email system could be construed to constitute an electronic communication service provider. *See* Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Dep't of Justice (DOJ)(2009), at 117-118, *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. If this interpretation of SCA were also applied to the definition of communication service providers for purposes of Section 702 – in

what is intended nor the way section 702 is applied. Rather, based on the legislative purpose for enacting section 702 (which is discussed below), the scope of "provider" under this law is widely understood to apply to companies that are actually in the business of providing communication services to others, rather than merely for their own corporate use. Significantly, PCLOB's Section 702 Report confirms that "FISA defines electronic communication service providers to include a variety of telephone, Internet service, and other communications providers."[20]

The interpretation that section 702 applies to companies in the business of providing communication services is further buttressed by text in section 702 that specifically contemplates that the communication services in question are those that are "provid[ed] to the target of the acquisition."[21] In other words, communications services that are provided by a company in the business of providing communication services (rather than essentially just using communication services).

---

rejection of the analysis here (notwithstanding the consensus that section 702 communications providers are a discrete set of communications companies) – it would not be fatal to the ultimate conclusion presented in this article because the fundamental thesis turns on authoritative text that prohibits intelligence agencies from targeting U.S. persons and persons located in the U.S. under section 702 and EO 12333.

DOJ's view is also instructive with regard to "remote computing services," *see id.* at 119-120 (emphasis added):

> The term "remote computing service" ("RCS") is defined by 18 U.S.C. § 2711(2) as "the provision to the public of computer storage or processing services by means of an electronic communications system." … Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65. For example, a service provider that allows customers to use its computing facilities in "essentially a time-sharing arrangement" provides an RCS. H.R. Rep. No. 99-647, at 23 (1986). A server that allows users to store data for future retrieval also provides an RCS. See Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 442-43 (W.D. Tex. 1993) (provider of bulletin board services was a remote computing service), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994). Importantly, an entity that operates a website and its associated servers is not an RCS, unless of course the entity offers a storage or processing service through the website. For example, an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into an RCS. See In re Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d at 310; see also United States v. Standefer, 2007 WL 2301760, at *5 (S.D. Cal. Aug. 8, 2007) (holding that e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users"). … [A] service can only be a "remote computing service" if it is available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example, Verizon is a provider to the public: anyone can obtain a Verizon account. (It may seem odd at first that a service can charge a fee but still be considered available "to the public," but this approach mirrors commercial relationships in the physical world. For example, movie theaters are open "to the public" because anyone can buy a ticket and see a show, even though tickets are not free.) In contrast, providers whose services are available only to those with a special relationship with the provider do not provide service to the public. For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "to the public" clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to "any member of the community at large").

[20] *Supra* n. 4 at 21.

[21] 50 U.S.C. 1881a(i)(A).

NSA's explanation of the reasons and need for section 702 confirms that companies subject to this authority are providers of "communication services based in the U.S.":

> "… as American internet and communications technology became globally dominant; people around the world started using American email systems and other applications. Our foreign intelligence targets were no exception, as they increasingly gravitated to communications services based in the U.S. As a result, if the government wanted to conduct electronic surveillance on a foreign target who was communicating overseas with another foreign target, it was increasingly the case that collection potentially fell within FISA's scope as the point of collection was often a service provider here in the U.S. In many such cases, the only way that the government could obtain the foreign intelligence it needed was to get a FISA order. In order to obtain those orders, the government had to prepare the same type of FISA application - a traditional Title I FISA application - that it would submit when the surveillance was targeted at a U.S. person. These traditional Title I FISA applications required the government to demonstrate "probable cause" to believe that the proposed target was a foreign power or agent of a foreign power and that the target was using or about to use the targeted facility (such as a telephone number or email address). As you all know, proving the existence to a federal judge of "probable cause" is hardly a trivial matter…. Congress's fix enabled the government to target for surveillance foreigners located outside the U.S. with the compelled assistance of U.S. service providers."[22]

The NSA's official summary of its various missions and authorities makes equally clear that section 702 applies to players in the U.S. "hub" for the "world's telecommunications system."[23]

Even more importantly, the Foreign Intelligence Surveillance Court (FISC) likewise understands that the U.S. government is authorized to acquire information under section 702 from, "Internet backbone carrier[s]," "from systems operated by providers of services," and "[t]raditional telephone communications."[24] The Court's recent 83-page decision approving the government's

---

[22] Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance Act, National Security Agency (2017), *available at* https://www.nsa.gov/news-features/speeches-testimonies/Article/1619167/judicial-oversight-of-section-702-of-the-foreign-intelligence-surveillance-act/ (emphasis added).

[23] "The principal application of this authority is in the collection of communications by foreign persons that utilize U.S. communications service providers. The United States is a principal hub in the world's telecommunications system and FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans." The National Security Agency: Missions, Authorities, Oversight and Partnerships, NSA Release No: PA-026-18 (Aug. 9, 2013), *available at* https://www.nsa.gov/news-features/press-room/Article/1618729/the-national-security-agency-missions-authorities-oversight-and-partnerships/.

[24] Mem. Op. and Order, FISC, at 9 (Dec. 6, 2019; released Sept. 4, 2020)(addressing section 702 2019 certification), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf. FISC Judge James E. Boasberg approved the U.S. government's certification under section 702, including targeting and minimization procedures. The Court discussed the NSA's obligation to provide an "explanation," and "review[] and evaluat[e] the sufficiency of [its] assessment that the target is a non-U.S. person location outside the U.S.: *Id.* at 16, 21. The Court also discussed changes to FBI targeting and information sharing procedures that "enhance the FBI's ability to research and evaluate whether a target is a U.S. person or in the United States." *Id.* at 10 (emphasis added).

2019 certification to use section 702 does not mention or provide implicit support for intelligence agencies attempting to target corporate email accounts.

Finally, even Max Schrems knows that communication service providers subject section 702 are the discrete set of companies in the business of providing such services. Indeed, his "none of your business" (NOYB) website identifies only about ten tech/telecom companies that are covered by section 702.[25]

2. Limitations on targeting that applys to protect data transfers to the U.S. under SCCs.

Under section 702, 50 U.S.C. 1881a(b), the U.S. government:

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States.

SCCs necessarily entail a contract between a data exporter in Europe and a data importer in the U.S.

Typically the exporter will be a U.S. corporation as will be the importer. The data importer, however, will always be a person located in the U.S. Accordingly, SCC data transfers to the U.S. are quintessentially U.S. person to U.S. person communications involving one person that is necessarily located in the U.S.

Thus, SCC transfers are manifestly not the type of foreign-foreign communications that section 702 was enacted to cover (as demonstrated in the prior section). Instead, they are U.S. person communications that the U.S. intelligence community "may not intentionally target" as specified in the statutory block quote above. For the avoidance of any question, there is no controversy at all about the fact that companies incorporated in the U.S. are "U.S. persons" for purposes of section 702. Indeed, FISA provides the following definition (18 USC 1801):

> "'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence …, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but

[25] *See* NOYB FAQs, *available at* https://noyb.eu/en/next-steps-eu-companies-faqs (providing "list of US providers that fall under these surveillance laws").

does not include a corporation or an association which is a foreign power …." [emphasis added]

Moreover, foreign affiliates of U.S. corporations may also be considered U.S. persons if most of its employees are U.S. citizens, though this is not beyond doubt. The NSA's "querying procedures"[26] under section 702 state the following:

> "An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence." [emphasis added]

3. Data collection conducted outside the U.S. outside the jurisdiction of U.S. laws and the Constitution may not target U.S. person data under EO 12333.

As indicated earlier, EO 12333 reserves the highest level of protection for U.S. persons, and would thus not be a suitable basis on which to target the transmissions to or from the U.S. by U.S. companies under SCCs.

The Order[27] very narrowly circumscribes the ability of U.S. intelligence agencies to target U.S. persons, including corporations and other U.S. companies:

> "The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.… Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General …. United States person means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." [emphasis added]

In its explanation of its mission and authorities,[28] the NSA describes its work under EO 12333 as involving foreign communications by foreign persons "wholly outside the United States":

> "Executive Order 12333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States. To the extent a person located outside the United

[26] "Querying Procedures… Pursuant to Section 702," NSA at 3 (2019; released Sept. 4, 2020), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Querying_17Sep19_OCR.pdf.
[27] *Supra* n. 3.
[28] *Supra* n. 23.

States communicates with someone inside the United States or someone inside the United States communicates with a person located outside the United States those communications could also be collected. Collection pursuant to EO 12333 is conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA. Intelligence activities conducted under this authority are carried out in accordance with minimization procedures established by the Secretary of Defense and approved by the Attorney General."

Thus, while there are no statutory prohibitions applicable to EO 12333 (since there are no statutory authorizations), it is subject (by presidential order) to the same U.S. person limiting principles as under section 702 – namely, that U.S. person communications or communications directed to persons located in the U.S. may not be targeted.[29]

4. Some steps companies relying on SCCs could take to ensure their data transfers are recognized as involving U.S. persons and persons located in the U.S. (in order that such data is not inadvertently targeted when passing through communications service providers).

Skeptical readers may question how the NSA, FBI or even the CIA could possibly know (and thus respect) that data transfers from Europe to the U.S. are transmitted pursuant to SCCs, and that such SCCs constitute U.S. person communications involving U.S. persons at one or both ends of the transfer, and certainly involve a person located in the U.S. on the receiving end?

Well, the answer is they have to know – they are intelligence agencies after all. Moreover, they are legally obligated to try very hard to know what communications they are targeting, collecting and querying. And, further, the sufficiency of their knowledge, explanations, research, and evaluation about the nature and status of the data transfers they target, collect or query will be carefully evaluated by agency lawyers, inspectors general, congressional committees, PCLOB, and federal judges.

That is, for example, exactly what Judge James Boasberg did in the FISC opinion he released in September 2020. The Court directly addressed the NSA's obligation to provide an "explanation," and "review[] and evaluat[e] the sufficiency of [its] assessment that the target is a non-U.S. person location outside the U.S." along with the FBI's procedures "to research and

[29] Note, too, that PPD-28's mandated protections for foreign persons also apply to surveillance under EO 12333. *See supra* n. 10. *See also* Statistical Transparency Report Regarding the Use of National Security Authorities Calendar Year 2019, Office of Civil Liberties, Privacy, and Transparency (2020)(" Non-U.S. persons also benefit from many of the protective rules prescribed by the targeting and minimization procedures. Under Section 702, collection is targeted (i.e., not bulk), and must be limited to non-U.S. person targets located outside the United States who are expected to possess, receive, and/or are likely to communicate foreign intelligence information that is specified in one of the FISC-approved certifications. *See* Status of Implementation of PPD28: Response to the PCLOB's Report, October 2018 at 9. Additionally, 'as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies' minimization and/or targeting procedures.' See Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of FISA (July 2, 2014) at 100. Moreover, as noted previously, PPD-28 regulates the IC's retention and dissemination of personal information of non-U.S. persons collected pursuant to Section 702."), at 13, *available at* https://www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf.

evaluate whether a target is a U.S. person or in the United States."[30] We can reasonably assume that intelligence agencies are particularly good at conducting such research and evaluation.

Indeed, NSA employees working on section 702 collections must receive special training toward this end:[31]

> "Before an analyst gains access to any NSA signals intelligence data, the analyst must complete specialized training on the legal and policy guidelines that govern the handling and use of the data. Additional training is required for access to Section 702 data. These annual mandatory training requirements include scenario-based training, required reading, and a final competency test. The analyst must pass this test before being granted access. Furthermore, if a compliance incident involves a mistake or misunderstanding of relevant policies, the analyst is re-trained in order to continue to have access to the data acquired pursuant to Section 702." [emphasis added]

In fact, the NSA is required to acknowledge and report on incidents where agency personnel exercise "insufficient due diligence … [that] impac[t] United States persons [and] involve[e] the tasking of facilities where the Government knew or should have known that at least one user of the facility was a United States person."[32]

Nonetheless, companies transferring data to the U.S. under SCCs should be sure to help the intelligence agencies recognize SCC "scenarios," and understand SCC data for what they are: communications transferred or received by a U.S. person or both, that are necessarily and inevitably intended for a recipient located in the U.S.

Some supplemental measures are suggested below. Implementing additional measures would help flag and signal that a company's SCC transfers to the U.S. may not be properly targeted by U.S. intelligence agencies. And if improper, inadvertent or incidental collection does occur, the intelligence agencies should be held accountable, and the company may even take corrective action.

Companies can keep this in mind while conducting their required assessments of their ability to comply with the requirements of SCCs as mandated by *Schrems II* and the European Data Protection Board (EDPB). In addition, companies could consider adopting other supplemental measures to more readily identify their SCC data transfers as "U.S. Person Communications" to assist U.S. intelligence agencies recognize the traffic as off-limits for 702 and 12333.

---

[30] *Supra* n 24. (emphasis added).
[31] "NSA Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702," NSA (2014) at 4, *available at* https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf.
[32] "SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE," Office of the Director of National Intelligence (Dec. 2019)(emphasis added), at 44, *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/19th%20Joint%20Assessment%20for%20702%20Dec%202019%20-%20Final%20for%20release%20(002)OCR.pdf.

In addition, companies could consider articulating or adopting some or all of these and other supplemental measures in their assessment or public privacy statements:

a. State whether or not they have ever received national security intelligence collection demands under 702 or 12333 with respect to EU data transferred to the U.S. under any Article 46 mechanism (i.e., SCCs, Privacy Shield, binding corporate rules, etc.).
b. Establish that company is not a communications service provider for purposes of Section 702.
c. Commit to challenging any 702 directive it in good faith believes is unauthorized.
d. Inform relevant communications service providers upon commencement of ECS or RCS service with them, and periodically thereafter, that communications emanating from the company's domain to a recipient in the U.S. is a U.S. person communication to a person located in the U.S.
e. Assert to the service provider that the company would challenge any 702 or 12333 directive purporting to collect the company's U.S.-bound communications from the EEA, and request that the service provider provide meaningful advance notice of any such attempted collection to the full extent permitted by law.
f. Mark SCC data transfers as "U.S. Person Communications/Transferred to Person in U.S."
g. State publicly in corporate privacy policies that data transfers to the U.S. pursuant to SCCs are U.S. person communications.
h. Export data from U.S. incorporated entities to the extent feasible.
i. Where appropriate in good faith, consider challenging 702 directives or EO 12333 collections of SCC data as unlawfully targeting U.S. person communications, or communications to a person located in the U.S.

Conclusion

One hopes that EU supervisory authorities, the European Data Protection Board, and Max Schrems will acknowledge that SCC data transfers to the U.S. do not pose the "surveillance" problem the CJEU thought. Given there is no empirical evidence that personal data transferred from the EU to the U.S. under SCCs has been the subject of actual surveillance by U.S. intelligence agencies, and that U.S. "national legislation" actually precludes targeting such transfers between U.S. companies, U.S. companies should be able to readily satisfy their self-assessment obligation under *Schrems II.* Ideally, EU member states could establish a body like PCLOB in the U.S., perhaps even on an ad hoc basis, that could confirm that data transfers under SCCs are simply not surveillance targets that infringe on the privacy rights of EU citizens—neither in practice nor in principle.