Transferring EU Data To US After New Contractual Safeguards

By **Alan Raul** (May 17, 2021)

Alan Raul

In light of new standard contractual clauses, or SCCs, to be issued shortly by the European Commission, as well as imminent new guidance from the European Data Protection Board, companies transferring personal data to the U.S. should consider taking steps to help ensure their data transfers are recognized as U.S. person communications.

This article sets forth possible text that companies could adopt as a supplemental measure to inform U.S. intelligence agencies that data transfers under SCCs are prohibited from being targeted.

By way of background, in its July 16 opinion in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, or Schrems II,[1] the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield framework that authorized the transfer of personal data from the European Economic Area to the U.S. The CJEU also expounded on the preexisting compliance requirements that arise from the SCCs as an alternative mechanism for such transfers and imposed onerous new obligations on their use.[2]

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.

Two specific authorities arose as the key considerations in this matter due to their historical assessment in the European Commission's Privacy Shield decision,[3] the validity of which was in question in Schrems II. Particularly troubling to the CJEU were Section 702 of the Foreign Intelligence Surveillance Act, "Procedures for targeting certain persons outside the United States other than United States persons,"[4] and Executive Order No. 12333 on U.S. intelligence activities.[5]

The CJEU appeared to believe that these surveillance authorities involved possible bulk collection of EU personal data that was executed with insufficient predication and overly broad targeting criteria, and further did not provide sufficient individual redress rights.[6]

However, under Section 702 of the FISA,[7] 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.

The National Security Agency, Federal Bureau of Investigation and the Central Intelligence Agency are legally obligated to know what communications they are targeting, collecting

and querying.

Furthermore, 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, privacy and civil liberties officers, the Privacy and Civil Liberties Oversight Board and federal judges sitting on the Foreign Intelligence Surveillance Court.

U.S. District Judge James Boasberg explained the intelligence agencies' legal responsibilities in a FISC opinion released in September 2020. He noted the NSA's obligation to provide an explanation and "review and evaluate 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 evaluate whether a target is a U.S. person or in the United States."[8]

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."[9]

Identifying Data Transfers to the U.S. as U.S. Person Communications

As expanded on below, an even more recent decision of the FISC, as well as a decision of the CJEU, support the thesis that U.S. intelligence agencies must take account of all available information surrounding SCC transfers to the U.S. and that the FISC's judicial review is more than adequate to enforce Section 702's targeting prohibitions.

Therefore, companies transferring personal data to the U.S. may wish to consider adopting the communication outlined below as a component of the self-assessment they are required to undertake under Schrems II, including potentially as a supplemental measure if deemed appropriate under such assessment. Specifically, companies should alert the intelligence agencies that their SCC transfers to the United States are U.S. person communications.

This measure would involve companies that are not electronic communication service providers[10] for purposes of FISA Section 702, sending a letter to the privacy and civil liberties officers[11] of the Office of the Director of National Intelligence, NSA, CIA and FBI — via the U.S. Department of Justice and the FBI Office of the General Counsel — and to the PCLOB, informing those agencies of the following facts and circumstances:

> Dear Sir or Madam:
>
> For purposes of targeting communications under Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S. Code § 1881a - Procedures for targeting certain persons outside the United States other than United States persons.
>
> We hereby inform you that communications of our Company to the United States may not properly be targeted under FISA Section 702 because they are U.S. person communications. Moreover, please be aware that our Company only transmits corporate-related communications to the U.S., and accordingly, we are not in the business of transmitting communications to the United States on behalf of the public or of third parties who are not related to our corporate business.
>
> Specifically, please be aware that we transmit communications containing personal data regarding our employees, customers, vendors, business partners, and other

> individuals or entities related to our business, to the United States from the European Economic Area (EEA) or United Kingdom (UK) via our Company's corporate email domain, shared file or hosting systems, remote computing or cloud services, and other communications modalities, and we do so pursuant to Standard Contractual Clauses (SCCs) [and/or Binding Corporate Rules] wherein the contractually designated (and actual) recipient of such personal data is a U.S. person (i.e., a company incorporated in the United States), and the persons actually receiving such personal data are located in the United States. [In addition, the entity transmitting such personal data from the EEA or UK to the U.S. is also a U.S. person by virtue of being incorporated in the United States, or is a subsidiary or wholly-owned affiliate of a U.S. person.]
>
> We respectfully bring this information to your attention so that you may be aware of and take into account the nature and status of our corporate communications for any targeting or tasking determinations implicating our communications.
>
> Thank you for your consideration of these facts and circumstances, and the corresponding legal factors.

There is reason to believe such a letter would be effective. In its November 2020 opinion, the FISC confirmed that U.S. national security agency targeting officials are obligated to inform themselves regarding the totality of circumstances relating to Section 702's prohibition against targeting U.S. person communications.

And the court's opinion demonstrates that it will thoroughly assess and adjudicate whether Section 702 targeting procedures and practices comply with the criteria and legal prohibitions of the statute.[12]

The FISC opinion confirms that the intelligence agencies do in fact implement, maintain and observe procedures designed to ensure that U.S. person communications are not targeted and that intelligence agencies targeting procedures satisfy those criteria.[13]

The court explained that the NSA is lead agency for targeting decisions and that it must make a foreignness determination considering the totality of the circumstances in order to comply with Section 702's prohibition on targeting U.S. persons.

In making such determinations, NSA reviews certain categories of information about the proposed target and evaluates the totality of the circumstances based on the information available with respect to that person.[14]

Furthermore, the FBI also reviews and evaluates the sufficiency of the NSA's explanation of its foreignness determinations and "runs certain checks of information in its possession in the course of that review and evaluation"[15] to determine the requested targeting "is in fact appropriate for tasking."[16] Indeed, the FBI, NSA and CIA are obligated to share information and coordinate to assure judicial approval of Section 702 certifications.[17]

In addition to such coordination on targeting and tasking, the NSA must also report to the Office of the Director of National Intelligence's Office of Civil Liberties, Privacy and Transparency regarding any incidents of noncompliance and incidents in which a person initially believed to be a non-U.S. person "is later assessed to be a United States person."[18]

Significantly, the court's "review of the sufficiency of Section 702 procedures is not limited

to the procedures as written, but also encompasses how they are implemented."[19]

While the CJEU appeared to disparage U.S. judicial oversight that did not involve individual redress in Schrems II, in the 2020 La Quadrature du Net decision, the CJEU itself endorsed the type of procedural review and safeguards provided by the FISC under Section 702. The CJEU has upheld a process that did not entail any requirement for, or even a meaningful possibility of, individual redress.

Specifically, EU member states were permitted to conduct "general and indiscriminate" and "sensitive" electronic surveillance, including collection of real-time traffic and location data, so long as "the Member State concerned is confronted with a serious threat to national security" and the surveillance "decision … is subject to effective review, either by a court or by an independent administrative body" in order "to verify … that the conditions and safeguards … are observed."[20]

No individual judicial redress was provided — only verification of applicable conditions and safeguards — just like the FISC under Section 702.[21]

While this CJEU decision was evaluating EU member state law, the principles the court applied to find European judicial review of electronic surveillance legally sufficient should be relevant by analogy to assessing the equivalence of the FISC's oversight under Section 702.

Importantly, the CJEU agreed to uphold what it viewed as significant interference with fundamental privacy and data rights:

> as long as there are sufficiently solid grounds for considering that the State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable and subject to meeting other requirements laid down in Article 52(1) of the [EU Charter of Fundamental Rights].[22]

Namely, such limitations may be sustained "if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[23]

Conclusion

Companies' ability to satisfy their self-assessment obligations under Schrems II should be enhanced by (1) FISA Section 702's prohibition against targeting U.S. person communications, (2) the supplemental measure of writing letters to inform U.S. intelligence agencies that companies' corporate SCC data transfers are U.S. person communications, and (3) the FISC's effective judicial review of Section 702 conditions and safeguards.

Alan Charles Raul is a partner at Sidley Austin LLP.

[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] For more detailed analysis of the issues discussed here, please visit: https://datamatters.sidley.com/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; and, https://www.lawfareblog.com/why-schrems-ii-might-not-be-problem-eu-us-data-transfers.

[3] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (C/2016/4176) (the "Privacy Shield Decision").

[4] 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.

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

[6] 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).

[7] 50 U.S.C. 1881a(b). Similar principles and restrictions apply under Executive Order 12333. For more detailed analysis of the issues regarding EO 12333, see https://datamatters.sidley.com/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; and, https://www.lawfareblog.com/why-schrems-ii-might-not-be-problem-eu-us-data-transfers.

[8] 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.

[9] "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant

To Section 702 of the Foreign Intelligtence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence," Office of the Director of National Intelligence (Dec. 2019), 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.

[10] The discrete companies that are electronic communication service providers for purposes of Section 702 could also send such a letter with respect to their own corporate data transfers, as distinct from the communications they transmit or host on behalf of their customers as part of their communications business.

[11] Note that exact titles for the privacy and civil liberties (PCL) officers at different agencies vary. See, e.g., https://www.nsa.gov/about/civil-liberties/about/#:~:text=The%20NSA%20Civil%20Liberties%20and,the%20Constitution%20and%20federal%20law (NSA); https://www.justice.gov/opcl (DOJ); https://www.fbi.gov/about/leadership-and-structure (FBI OGC maintains a "Privacy and Civil Liberties Unit"); https://www.dni.gov/index.php/ctiic-who-we-are/leadership/197-about/organization/office-of-civil-liberties-privacy-and-transparency (ODNI); https://www.cia.gov/about/organization/privacy-and-civil-liberties/#:~:text=The%20Privacy%20and%20Civil%20Liberties,activities%20as%20required%20by%20law (CIA); and, https://www.pclob.gov/ (PCLOB).

[12] Section 702 2020 Certification, U.S. Foreign Intelligence Surveillance Court Opinion (Nov. 18, 2020; declassified and released April 26, 2021), https://assets.documentcloud.org/documents/20691797/2020_fisc-cert-opinion_10192020.pdf.

[13] Id. at 7.

[14] Id. at 8 (internal quotes omitted).

[15] Id. at 9.

[16] Id. at 10.

[17] Id.

[18] Id.

[19] Id. at 35.

[20] La Quadrature du Net, Judgment of the Court (Grand Chamber), Court of Justice of the European Union (6 Oct. 2020; rectified 16 Nov. 2020), https://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=en.

[21] The observation that Section 702 criteria and judicial oversight by the FISC would easily satisfy the CJEU's framework in La Quadrature du Net is not offered to relitigate or call into question the merits of Schrems II. Rather, it is offered to point out that, depending on the circumstances, even the CJEU has acknowledged that judicial review can be effective in protecting substantive rights without recourse to individual judicial redress. (Indeed, the CJEU approved the procedure without individual redress even though the electronic surveillance in question was "general and indiscriminate," "real-time," "particularly

"sensitive" and "intrusive." The Court justified the sufficiency of generalized oversight because "the Court must strike a balance between the various interests and rights at issue," and "the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights ….").

[22] See also EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020 ("European Essential Guarantees Recommendations") pp. 34.

[23] In light of the substantial overlap between membership of the EU and EEA, on the one hand, and the North Atlantic Treaty Organization, on the other, there can be no doubt that combatting terrorism along with the U.S., and promoting mutual national security, is an objective of general interest recognized by the EU. In fact, to this day, the only time NATO's provision for "collective defence" (Article 5) has been invoked was upon petition of the U.S. following the 9/11 terrorist attacks. (Article 5 stipulates that "[t]he Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all….") And, as the CJEU acknowledged in La Quadrature du Net, overlap in treaty membership is relevant to the Court's assessment of the legitimacy of measures related to electronic surveillance that may be perceived to encroach on fundamental rights:

In that regard, the Council of Europe's Convention on Cybercrime of 23 November 2001 (European Treaty Series– No.185), which was signed by the 27 Member States and ratified by 25 of them and has as its objective to facilitate the fight against criminal offences committed using computer networks, provides, in Article14, that the parties to the convention are to adopt, for the purpose of specific criminal investigations or proceedings, certain measures concerning traffic data already stored, such as the expedited preservation of that data. In particular, Article16(1) of that convention stipulates that the parties to that convention are to adopt such legislative measures as may be necessary to enable their competent authorities to order or similarly obtain the expedited preservation of traffic data that has been stored by means of a computer system, in particular where there are grounds to believe that that data is particularly vulnerable to loss or modification.