Supplementing SCCs to solve surveillance shortfalls

Aug 19, 2020 Save This ()

Marc Zwillinger
IAPP Member Contributor (/about/person/0011a00000DlDG2AAN)

Mason Weisz
Nonmember Contributor (/about/person/0011a00000DlIreAAF)

Kandi Parsons
Nonmember Contributor (/about/person/0011a00000DlO3iAAF)

By invalidating the EU-U.S. Privacy Shield but not rejecting wholesale the use of standard contractual clauses to transfer data to the U.S., the Court of Justice of the European Union in "Schrems II" left open the possibility that such transfers could continue. However, it emphasized that exporters and importers may need to adopt additional safeguards when using SCCs to ensure an adequate level of protection for personal data transferred to the U.S.

Until now, commentators have seemed unsure as to what those safeguards might be or how they can address potentially irredeemable flaws in the U.S. surveillance system. In this piece, we detail a proposed solution consisting of technical measures, supplemental clauses and exit strategies.

Our solution can work because the CJEU decision was — at its core — based on three essential holdings. First, Section 702 (https://www.law.cornell.edu/uscode/text/50/1881a) of the Foreign Intelligence Surveillance Act (https://www.law.cornell.edu/uscode/text/50/chapter-36) provides no effective limitations on the power of the U.S. government to implement surveillance programs for foreign intelligence gathering and, therefore, fails the test of proportionality.

Second, neither Section 702 nor the government's surveillance activities under Executive Order 12333 (https://dodsioo.defense.gov/Library/EO-12333/) adequately limit the surveillance to what is strictly necessary as required by the EU General Data Protection Regulation, because they allow for forms of bulk surveillance.

And third, non-citizens lack adequate judicial redress against the USG under these surveillance authorities.

Although it is impossible to solve the judicial redress issue without U.S. structural reform, such redress only becomes necessary if the data at issue is, in fact, collected by the USG under the relevant surveillance programs. Moreover, where the likelihood of USG acquisition is very low, the transfer should satisfy the essential equivalence standard — for the same reason that Article 32 of the GDPR does not require perfect data security but rather a level

are designed to be used in jurisdictions that have not achieved an adequacy determination.

Accordingly, the questions remain: What supplemental measures can appropriately reduce the risk of interception under EO 12333 or Section 702 of FISA? In other words, in light of "Schrems II," how can the parties find, prior to any transfer, that there is, in fact, an “adequate level of protection” for personal data in the importing jurisdiction and that the recipient can comply with the standard data protection clauses transferring personal data to that third country?

The key is found in footnote 2 of the controller-to-processor SCCs, which is that laws that require data to be turned over to governmental entities do not invalidate the SCCs where, in a democratic society, they “constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offenses or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.”

The CJEU found the availability of surveillance and data acquisition under 12333 and Section 702 of FISA fails this test. If the data transferred to the U.S. cannot be obtained under these surveillance programs, then the programs shouldn’t impede the transfer — even without enhanced judicial redress for non-citizens. Indeed, adequate judicial redress for non-U.S. people has not always been available for certain forms of standard criminal process that generally are perceived to satisfy the standard in the footnote — and nothing about the decision suggests that standard criminal process alone would prevent the use of SCCs.

Defeating EO 12333 interceptions

With regard to EO 12333, the chief evil cited in the CJEU opinion was bulk surveillance and specifically the ability of the NSA to access data "in transit" to the U.S. by accessing underwater cables on the floor of the Atlantic and to collect and retain such data before arriving in the U.S. (p. 63). This issue can be solved through a combination of technical measures and contractual promises.

First and foremost, EO 12333 allocates surveillance responsibility within the USG and provides it with the authority to conduct its own surveillance activities but provides no mechanism for forcing importers to assist the government. Thus, importers can contractually commit to not voluntarily assist the government in conducting operations under EO 12333.

Second, interceptions can be defeated through technical measures, like, for example, sufficiently strong encryption such that the USG cannot understand the substance of the data without the key, which it cannot compel importers to produce under 12333. If the USG cannot understand the substance of the data, there is no risk to the data subjects reflected in the data, and this particular safeguard can be considered adequate with respect to 12333. Thus, a commitment to encrypting all data in transmission and not voluntarily assist the government in its conduct of 12333 activities should defeat one of the core deficiencies cited in the CJEU decision. (Other technical measures that defeat the USG’s ability to understand the data without cooperation would also work.)

Surmounting Section 702

The CJEU decision fails to recognize the limited nature of Section 702 surveillance.

First, not all providers are eligible to receive a “directive” (an order that leads to the USG’s acquisition of data) under 702. Only electronic communication service providers (https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=50-USC-1989240790-1235549439&term_occur=999&term_src=title:50:chapter:36:subchapter:VI:section:1881a) are eligible. Importers that are not ECSPs can, therefore, provide assurances of ineligibility and agree to fight any 702 directive. And even if the

decryption/reidentification required the exporter's cooperation.

As for importers that are ECSPs (in whole or in part), the government only uses Section 702 where there is a repeated need for multitarget collection without the inefficiency of going to the FISA court for individual surveillance orders via a procedure that has greater judicial oversight.

Indeed, at the time of the Snowden leaks, it was reported that fewer than 10 companies were receiving 702 orders. Even if that number has doubled or tripled, it would be an insignificant percentage of the more than 5,300 companies that may be moving from Privacy Shield to SCCs, much less the entire field of importers who rely on SCCs.

Thus, nearly all of them could promise that they have received no process under 702, and they can keep making that promise unless and until they receive a directive. Others can promise that the number of affected users under all national security process is published in their transparency reports, which exporters can compare to the number of overall data subjects about whom they collect data to make an accurate risk assessment. Where the chance of 702 collection identified through this reporting is sufficiently low (say, less than 1%, which is far lower than the chance of a data breach), an exporter may be able to justify continued exports.

Exit strategy: The potentially unkeepable promise

Of course, a provider that makes any sort of promise related to Section 702 surveillance as part of a package of supplemental clauses may be unable to keep that promise someday.

However, the SCCs already contemplate that situation, under C2P SCC Clause 5, and controller-to-controller SCC Clause II(c), an importer is required to notify an exporter of its inability to comply with SCCs, enabling the exporter to suspend and terminate the contract. An importer could similarly agree to notify an exporter that it will no longer be able to comply with all of its SCC and supplementary promises, without directly notifying the exporter which specific promise it can no longer keep, and offer the same suspension/termination right. Although explicit notification of the receipt of a directive is legally prohibited, a notification that the importer will no longer be able to comply with a set of promises would not violate non-disclosure restrictions, especially where it could be equally likely that the inability to comply was due to something else, such as a failure with the importer's service provider.

And because a 702 directive is a demand for the importer's cooperation — and not some sort of notice to the importer that data already has been acquired — importers can expect to provide their warning to the exporter in advance of any actual disclosure.

Service providers are tricky

The CJEU decision and Article 44 of the GDPR indicate that the assessment of the adequacy of protection must consider the importer's transfers of data to subprocessors or other service providers (among other third parties).

Notably, under Clauses 4(i) and 11(1) of the C2P SCCs, an importer agrees to flow down its SCC obligations to its subprocessors, who must provide "at least the same level of protection for the personal data and the rights of data subject as the data importer." C2C SCCs are less proscriptive, but it is hard to argue that an importer provides adequate protection if it passes the data to a U.S.-based service provider without addressing the risks identified in the CJEU decision. Just as supplementary provisions to the SCCs, such as those outlined above, may let importers adequately protect data transferred to the U.S., importers may be able to address onward transfer risks to service providers by doing one or more of the following: (1) using technical safeguards such as encryption to prevent the

requirement may be unworkable because, for example, a non-ECSP cannot be expected to flow down a non-ECSP rep to its service providers who are ECSPs); (3) for eligible transfers, relying on a derogation set forth in Article 49 of the GDPR; and/or (4) using service providers located in the European Economic Area or an adequate jurisdiction.

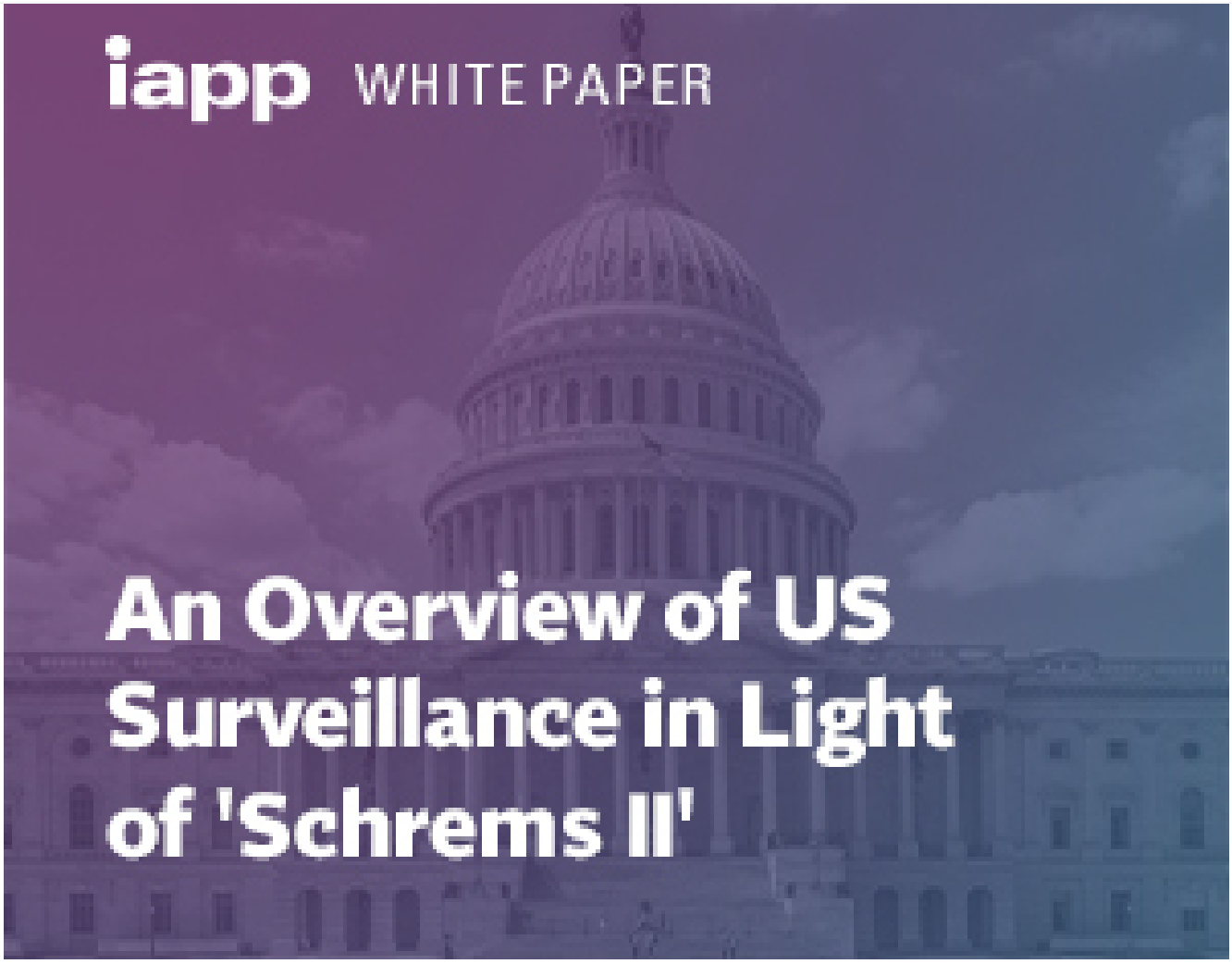
Option two, which for some importers is the least obtainable, could become easier if supervisory authorities signal support for the solution proposed in this article, thereby hastening its widespread adoption.

Conclusion

The irony of utilizing supplemental clauses to assist in the transfer of data to the U.S. is that EU data is sometimes better protected against the USG when it is imported into the U.S. than when it is kept outside the U.S. When data is outside the U.S. borders and doesn't pertain to U.S. citizens, U.S. surveillance authorities allow the government to operate in an arguably unrestricted manner to obtain such data subject only to capability limitations. Only when the data is imported by U.S. companies does the mandate of U.S. intelligence agencies become circumscribed by U.S. legal authority, including under EO 12333 and FISA.

Thus, inside the U.S., the USG's power is curtailed and subject to judicial oversight and the often-effective pushback by U.S. technology companies. Nevertheless, the use of the safeguards described in this article should — to the maximum extent possible without requiring changes to the U.S. judicial redress regime — allow for continued cross-border data transfers.

Photo by Duangphorn Wiriya on Unsplash



(https://iapp.org/resources/article/overview-us-surveillance-light-of-schremsii/)

The purpose of this white paper is not to argue for the validity or invalidity of any particular surveillance mechanism, but rather to provide a neutral, unclassified summary of the law and authorities in this area.

Click to view (https://iapp.org/resources/article/overview-us-surveillance-light-of-schremsii/)

GDPR Genius

(https://iapp.org/resources/article/gdpr-genius/)

This interactive tool provides IAPP members ready access to critical EU General Data Protection Regulation resources — enforcement precedent, interpretive guidance, expert analysis and more — all in one location.

View here (https://iapp.org/resources/article/gdpr-genius/)

Approved CIPM, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPT Credits: 1

SUBMIT FOR CPES (/CERTIFY/CPE-SUBMIT/)

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200