The Impact of Schrems II on the Modern Multinational Information Security Practice, Part 1

The Potential Disruption to International Commerce

The transfer of personal data out of the European Union (EU) to nations around the world takes place tens of thousands of times every day, and it has been occurring for so long that it has largely become routine business. Typically made in a commercial context, the data may involve personal travel information, employee healthcare data, privileged communications or any number of other types of personal data. Until the summer of 2020, the legal protocols for the movement of personal data out of the EU were well understood and widely accepted by multinational organizations. However, on 16 July 2020, the Court of Justice of the EU (CJEU) rendered what is likely to be its most disruptive decision to international commerce to date.

In case C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*[1] (Schrems II), the CJEU invalidated the US-EU Privacy Shield Program, a data transfer protocol that had been negotiated over the course of two and a half years by the US Department of Commerce and the European Commission. In doing so, it threw into doubt the legality of transatlantic personal data transfers for thousands of organizations, while offering a murky path forward. While the CJEU completely invalidated one protocol, Privacy Shield, it largely upheld the validity of another, known as standard contractual clauses (SCCs). SCCs may continue to be used to legitimize the transfer of personal data out of the EU, but the CJEU stated that "supplementary measures" now need to be implemented for transfers to countries where electronic surveillance puts personal data at risk and if a given country does not offer effective redress to EU people (data subjects) to enforce their rights. In particular, two legal instruments that make legal the gathering of electronic intelligence by the US intelligence community, Section 702 of the US Foreign Intelligence Surveillance Act (FISA) and US Executive Order 12333, were cited by the Schrems II order as particularly threatening to the rights of EU people.

Scott M. Giordano, JD, CISSP, IAPP FIP
Is an attorney with more than 20 years of legal, technology and risk management consulting experience. He is vice president, corporate privacy and general counsel at Spirion, where he serves as a subject-matter expert on multinational data protection and its intersection with technology, export compliance, internal investigations, information governance and risk management. Prior to joining Spirion, he served as director of data protection for Robert Half Legal and established the global privacy program for Esterline Technologies Corporation. During his career, Giordano has held senior positions at several legal technology firms and is co-inventor of Intelligent Searching of Electronically Stored Information. He taught the first law school course anywhere on electronic evidence and ediscovery.

> "SCHREMS II MAY BE THE MOST IMPORTANT LEGAL DECISION ABOUT WHICH MOST IT PROFESSIONALS LIKELY HAVE NEVER HEARD."

Data protection professionals are now tasked with making sense of what little guidance the CJEU offered and leveraging the necessary expertise to enable continued personal data transfers out of the EU. Although the decision received significant attention in the privacy space, it went largely unnoticed elsewhere. In fact, Schrems II may be the most important legal decision about which most IT professionals likely have never heard. Undoubtedly, the decision will change modern information security practice for professionals inside and outside of the EU.

Transferring Personal Data Out of the EU, Pre-Schrems

The EU promulgated its first comprehensive data protection regime in October 1995. The EU Data Protection Directive 95/46/EC thus became the principal data protection regime for the EU until the EU General Data Protection Regulation (GDPR) replaced it in May 2018.[2] Under the Directive, there were three ways to legally move personal data from the EU to the United States (US), a nation whose laws did not (and still do not) offer adequate (i.e., essentially equivalent to that of the EU) protection to data subjects:

1. SCCs—These are sets of standard clauses governing data transfers out of the EU to nations that have not received a prior ruling from the European Commission (EC) that their laws offer adequate protections to EU personal data. Using the SCCs, the organization (referred to as a data controller by the GDPR) that is receiving the personal data in a nonadequate nation is agreeing contractually with the organization transferring it to protect those data according to the mandates described in the clauses. Typically, SCCs were and are still used as part of a data processing addendum to a larger contract. An appendix to the SCCs contains a list of technical and organizational security controls that the importing organization stipulates to follow.3 Draft updates to the SCCs were made by the EC in light of the Schrems II decision and published in November 2020.
2. Binding corporate rules—Binding corporate rules (BCRs) are specially agreed upon SCCs for a group of related enterprises, such as a parent enterprise and its subsidiaries scattered around the world, or for multiple locations of a global enterprise. Salesforce, for example, has negotiated BCRs for its cloud environments so that data can flow freely between the clouds.4 One enterprise develops the draft rules and submits them to an EU data protection authority (now called a supervisory authority) for approval. Once approved, the BCRs govern the movement of personal data among the entity or group of enterprises. Thus, further involvement of the authority is not necessary unless the enterprises want to change how the personal data are processed.
3. Safe Harbor program—This program is an agreement established between the US Department of Commerce and the EC in 2000 as a means of moving personal data from the EU to the US.5 Under the program, US enterprises that wished to import EU personal data would self-certify that they are compliant with the program's requirements, which includes notice and choice given to data subjects and data security requirements. The enterprises were listed in a directory published by the US Department of Commerce and were allowed to advertise their compliance on their websites and elsewhere. The Safe Harbor program was enforced by the US Federal Trade Commission (FTC).

Those US enterprises that chose Safe Harbor as a transfer mechanism likely did so because it was relatively simple and cost-effective. They needed only to conduct an internal review for compliance with the principles of the program, make any needed changes and self-certify. However, all of that changed in the wake of Edward Snowden's disclosures related to surveillance operations conducted by the US National Security Agency (NSA) in June 2013.[6] Among the revelations was a program called PRISM,[7] which involved the NSA tapping into the communications of Internet service providers such as Microsoft, Google, Yahoo and Facebook and harvesting personal data.[8] Facebook was forwarding data about its users to the

NSA "for reasons of espionage, national security and other matters."[9]

As a result, Austrian privacy activist Maximilian Schrems, a Facebook user, filed a complaint with the Data Protection Commissioner of Ireland against Facebook Ireland Ltd. The essence of Schrems's argument was that there is no US adequacy under the program if the government can circumvent the Safe Harbor program by asking US enterprises to send EU personal data without the consent of the data subject and without any possibility of redress in US courts. However, the Data Protection Commissioner did not find any merit to the complaint and, after Schrems challenged its decision in the Irish courts, the matter was referred to the CJEU in June 2014.

On 6 October 2015, the CJEU invalidated the Safe Harbor program upon review, citing two fatal problems with it: The data in question were subject to "legislation permitting the public authorities [in the US] to have access on a generalized basis to the content of electronic communications,"[10] and EU data subjects did not have "an effective remedy before a tribunal" in the US.[11] This legislation is the US Foreign Intelligence Surveillance Act of 1978 (FISA), which authorizes "electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power."[12]

> "THE SNOWDEN REVELATIONS WERE HAVING A SUBSTANTIAL (AND LIKELY UNFORESEEN) IMPACT ON INTERNATIONAL COMMERCE."

Schrems cited a post-9/11 amendment to FISA that addresses surveillance against persons outside of the US in his complaint to the Commissioner. According to a definitive account of the Schrems saga, the CJEU's ruling should have been the end of the matter.[13] However, in November 2015, the Commissioner informed Schrems that the ruling was irrelevant *vis-à-vis* his earlier complaint because Facebook had relied on SCCs for its importation into the US, not Safe Harbor.[14] Although the legitimacy of Safe Harbor as a data transfer mechanism was resolved, the legality of Facebook's transatlantic transfers of personal data was not. Schrems amended his complaint to address Facebook's use of SCCs and potentially other data transfer mechanisms.[15]

The Road to Schrems II

Almost immediately after the invalidation of the Safe Harbor program, negotiators at the US Department of Commerce and the EC accelerated discussions of a replacement for Safe Harbor. On 12 July 2016, the EC deemed that replacement, the EU-US Privacy Shield Framework, adequate to enable data transfers under EU law,[16] and US-based enterprises began self-certifying under the new program's mandates. Meanwhile, by May 2016, the amended Schrems complaint had made its way to the Irish High Court, wherein Facebook argued that since Privacy Shield passed EC scrutiny in terms of US surveillance laws vs. EU fundamental rights, transfers under SCCs should also remain legitimate.[17] The High Court listened to testimony on the matter[18] from both sides and found that the US government had engaged in "mass indiscriminate processing of data" and issued a referral of the entire matter, including 11 questions, to the CJEU for a preliminary ruling.[19] The CJEU would later cite the findings of fact by the Irish High Court extensively in its ruling.

The Schrems II Decision

On 16 July 2020, the CJEU handed down what would become known as Schrems II. The decision both invalidated Privacy Shield and called into question data transfers using SCCs. Moreover, there was no grace period for data exporters to make changes—they would have to resolve any legitimacy questions about data transfers immediately. Once again, the Snowden revelations were having a substantial (and likely unforeseen) impact on international commerce.

Schrems II cited one US law and two legal instruments authorizing the gathering of intelligence on non-US persons by the NSA and other agencies within the US intelligence community and law enforcement agencies. The

decision alleges that there are shortcomings in these laws insofar as they do not offer non-US persons meaningful ways to challenge their application in US courts. The legal mechanisms cited include:

- **Executive Order 12333**—Executive Order 12333 was issued by US President Ronald Reagan in 1981 and expanded the US intelligence community's ability to obtain electronic intelligence by "accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA."[20] In doing so, such "upstream" collection of personal data from non-US persons defeats the opportunity to offer protection to such data offered by the FISA Court (FISC)—and, presumably, opportunities to protect the confidentiality of such data by the data exporter before it reaches the importer. In fact, one program cited by Snowden that ran under the auspices of 12333 was itself called UPSTREAM.[21]
- **FISA § 702**—FISA was first promulgated in 1978 and was designed only to protect US citizens. In the years following the 9/11 attacks, the need to address changes in technology and to speed up the ability to target non-US persons led to the passage of the FISA Amendments Act of 2008.[22] Changes to FISA, found in § 702, included the removal of the FISC's jurisdiction over the selection of individuals targeted by law enforcement and intelligence agencies and the degradation of the legal threshold from one of "probable cause" to one of "reasonably believed to be located outside the United States[.]" The Irish High Court, in its referral, stated that because the FISC only approves intelligence gathering programs, rather than addressing whether individuals are properly targeted, § 702 "does not indicate any limitations on the power it confers to implement surveillance programs for the purpose of foreign intelligence[.]"[23]
- **Presidential Policy Directive 28**—Presidential Policy Directive 28 (PPD-28) was issued by US President Barack Obama on 17 January 2014, some eight months after the Snowden revelations. PPD-28 purports to require the US intelligence community to minimize the collection of the personal information of non-US persons. However, the Irish High Court explicitly found that PPD-28 offers insufficient protection for the personal data of those persons, stating that "PPD-28 does not grant data subjects actionable rights before the courts against the US authorities."[24]

> "IT IS FOR THE DATA CONTROLLER OR PROCESSOR TO PROVIDE 'APPROPRIATE SAFEGUARDS' TO PROTECT THE DATA IN THE TRANSACTION."

The Invalidation of Privacy Shield

Looking at the totality of these three legal instruments and the resultant lack of ability of non-US persons to effectively challenge them in US courts, the CJEU invalidated the Privacy Shield program, stating that:

> *[T]he Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter [of Fundamental Rights of the European Union], contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights.*[25]

The CJEU later concluded that:

> *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.*[26]

And with that, Privacy Shield was no more.[27]

"Additional Safeguards" Putting US Enterprises in a Tough Spot

When the Irish High Court referred the second Schrems complaint to the CJEU, it did so by asking for a preliminary ruling on 11 questions, nearly all of which addressed the validity of SCCs. Since the Schrems I decision, the EU both brought into force and began enforcement of the GDPR. Articles 44–50 of the GDPR address the transfer of personal data outside the EU, and, in particular, Article 46 addresses the use of legal agreements to effectuate that transfer "if the controller or processor has provided appropriate safeguards[.]"[28] SCCs are referred to in this article as "standard data protection clauses."[29]

In answering the referred questions on SCCs, the CJEU held that the European Commission (which approved the SCCs originally) does not have to investigate the adequacy of the level of data protection ensured by potential non-EU destination countries for EU personal data. Instead, it is for the data controller or processor to provide "appropriate safeguards" to protect the data in the transaction. The Court then discussed several variations of this "safeguards" theme, three of which include:

1. "The possibility for the controller to use standard data-protection clauses adopted by the European Commission should not prevent it from adding other clauses or additional safeguards and states. The controller should be encouraged to provide additional safeguards that supplement standard data protection clauses."[30]
2. "In so far as those standard data protection clauses cannot...provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection."[31]
3. "It is therefore, above all,...to verify, on a case-by-case basis and, where appropriate...whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."[32]

> "DATA PROTECTION PROFESSIONALS ARE NOW TASKED WITH HAVING TO DETERMINE WHAT CONTROLS QUALIFY AS MEETING THIS NEW MANDATE AND TO DO SO LARGELY BY THEMSELVES."

What is remarkable about these holdings is that nowhere in the Schrems II decision does the Court offer examples of what qualifies as a potentially viable safeguard. Such measures could be technical or organizational or perhaps a combination of the two. The implication is that the safeguards may need to be designed to defeat or slow the collection capabilities of a state intelligence agency. What is apparent from the decision is that the onus of identifying and implementing safeguards that meet this requirement is now the responsibility of an organization's data protection professionals and its legal counsel. In this respect, Schrems II is not a recipe for clarity or consistency; in fact, it has injected considerable uncertainty into business operations.

Conclusion

The Schrems II decision has called into question the legality of the transfers of personal data from the EU to the US and other nations. It did so by invalidating one data transfer protocol, the Privacy Shield Program, and belaboring another, SCCs, with the necessity of supplementary measures to currently employed cybersecurity controls. The CJEU sees the prospect of electronic surveillance by US intelligence agencies of transatlantic data transfers as posing such a threat to the rights of EU people that measures apparently designed to frustrate such surveillance are merited. Data protection professionals are now tasked with having to determine what controls qualify as meeting this new mandate and to do so largely by themselves, owing to the CJEU's lack of guidance. Furthermore, those professionals have to make this

decision in short order, given that the CJEU's decision was effective immediately upon being handed down. This combination of lack of legal guidance and the need to immediately change an organization's current data protection practice is all but unprecedented. It may necessitate a complete rethinking of how practitioners approach data protection in the context of cross-border data transfers. "The Impact of Schrems II on the Modern Multinational Information Security Practice, Part 2" will discuss the response from the European Data Protection Board (EDPB), a data protection law enforcement agency, and what measures data protection teams can take now to minimize the impact to their organizations.

Endnotes

1 Court of Justice, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, Case C-311/18, 16 July 2020, *http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3705396*

2 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), *https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en*

3 Google, "Google Cloud Platform: EU Model Contract Clauses," Google Cloud Platform Terms, USA, 2018, *https://cloud.google.com/terms/eu-model-contract-clause*

4 Salesforce, *Salesforce's Processor Binding Corporate Rules for the Processing of Personal Data*, June 2021, *https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/Salesforce-Processor-BCR.pdf*

5 2000/520/EC: Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000, *https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520*

6 Gellman, B.; "U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program," *The Washington Post*, 7 June 2013, *https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html*

7 IC Off the Record, "PRISM/US-984XN Overview," April 2013, *https://nsa.gov1.info/dni/prism.html*

8 Electronic Privacy Information Center (EPIC), "EPIC v. DOJ – PRISM," *https://epic.org/foia/doj/olc/prism/*

9 Schrems, M.; "Complaint Against Facebook Ireland Ltd—23 'PRISM,'" 25 June 2013, *www.europe-v-facebook.org/prism/facebook.pdf*

10 European Court of Justice (ECJ), *Maximillian Schrems vs. Data Protection Commissioner*, Case C-362/14, 6 October 2015, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362*

11 *Ibid.*

12 Federation of American Scientists (FAS), *Foreign Intelligence Surveillance Act*, USA, 1978, *https://fas.org/irp/agency/doj/fisa/*

13 De La Torre, L. F.; "Schrems and the Future of EU-US Data Transfers (or Lack Thereof…)," *Medium*, 30 June 2019, *https://medium.com/golden-data/schrems-and-the-future-of-eu-us-cross-border-data-transfers-13970bf500b6*

14 *Ibid.*

15 *Ibid.*

16 Privacy Shield Framework, "Privacy Shield Overview," *https://www.privacyshield.gov/program-overview*

17 *Ibid.*

18 Gorski, A.; "EU Court of Justice Grapples With U.S. Surveillance in Schrems II," 26 July 2019, *https://www.justsecurity.org/65069/eu-court-of-justice-grapples-with-u-s-surveillance-in-schrems-ii*

19 *Op cit* Court of Justice

20 *Ibid.*

21 The National Security Agency (NSA), "PRISM/US-984XN Overview," IC Off the Record, April 2013, *https://nsa.gov1.info/dni/prism.html*

22 *Op cit* Federation of American Scientists

23 *Op cit* Court of Justice

24 *Ibid.*

25 *Ibid.*

26 *Ibid.*
27 As of this writing, the Irish Hight Court has denied Facebook's challenge to a September 2020 order by the Irish Data Protection Commissioner to suspend data transfers from the European Union to the United States.
28 Intersoft Consulting, Art. 46 GDPR, Transfers Subject to Appropriate Safeguards, Belgium, 2018, *https://gdpr-info.eu/art-46-gdpr/*
29 *Ibid.*
30 *Op cit* Court of Justice
31 *Ibid.*
32 *Ibid.*