"CONTRACTING OUT" HUMAN RIGHTS IN INTERNATIONAL LAW: SCHREMS II AND THE FUNDAMENTAL FLAWS OF U.S. SURVEILLANCE LAW

GENNA CHURCHES AND MONIKA ZALNIERIUTE

(2020) Harvard International Law Journal Online
[2020] *UNSWLRS* 44

UNSW Law
UNSW Sydney NSW 2052 Australia

"CONTRACTING OUT" HUMAN RIGHTS IN INTERNATIONAL LAW: *SCHREMS II* AND THE FUNDAMENTAL FLAWS OF U.S. SURVEILLANCE LAW

GENNA CHURCHES* AND MONIKA ZALNIERIUTE†

Abstract

In the midst of the COVID-19 pandemic, on July 16, 2020, the Court of Justice of the European Union ("CJEU") in Luxembourg handed down a long-awaited judgement on international data transfers in the *Schrems II* case. The Court found U.S. law does not provide the "essentially equivalent" protection for personal data to that guaranteed by EU law, and invalidated the key mechanism for EU-United States data transfers, Privacy Shield, for the *second* time in a decade. The CJEU generally upheld the validity of another legal basis for international data transfers—Standard Contractual Clauses ("SCCs") but implied these clauses are *not* an avenue for continued transfers of personal data from the EU to the United States. *Schrems II* is a win for human rights in the EU and beyond, yet, the long-term political impact of this judgement in securing human rights in the digital economy is less certain in light of the $7.1 trillion transatlantic economic relationship at stake. The U.S. government maintains that the protection under its national security laws "meets" and "exceeds" the safeguards "in foreign jurisdictions, including Europe," suggesting that structural changes in the U.S. legal system are unlikely. Instead, the European Commission ("EC") and U.S. Department of Commerce may soon carve out another solution for EU companies to "contract out" the protection for human rights where public authorities are unwilling to ensure it.

Keywords

Data protection, privacy, GDPR, international data transfers, human rights, international law, contracts, Privacy Shield, Schrems, Facebook, national security, surveillance, PRISM, EU, USA.

Citation

G. Churches and M. Zalnieriute, "'Contracting Out" Human Rights in International Law: Schrems II and the Fundamental Flaws of the US Surveillance Laws,' Harvard International Law Journal Online, 2020 <https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law/

* PhD Candidate, UNSW Law Sydney, Australia and Member of the Allens Hub for Technology, Law & Innovation, UNSW Sydney, Australia; g.churches@unsw.edu.au.

† Senior Lecturer, School of Law, Macquarie University, Sydney, Australia, monika.zalnieriute@mq.edu.au; and a Visiting Fellow UNSW Law, Sydney, Australia.

INTRODUCTION

In the midst of COVID-19 pandemic, on July 16, 2020, the Court of Justice of the European Union ("CJEU") in Luxembourg handed down a long-awaited judgement on international data transfers in the *Schrems II* case. The European Union ("EU") Court found that U.S. law does not provide the "essentially equivalent" protection for personal data to that guaranteed by EU law, and therefore invalidated the key mechanism for EU-United States data transfers—this time known as Privacy Shield—for the *second* time in a decade. While the CJEU generally upheld the validity of another legal basis for international data transfers—Standard Contractual Clauses ("SCCs"), the Court also implied that these clauses are not an avenue for continued transfers of personal data from the EU to the United States.

Schrems II is a win for human rights in the EU and beyond, yet, the long-term political impact of this judgement in securing human rights in the digital economy is less certain in light of the $7.1 trillion transatlantic economic relationship at stake. Until now, U.S. companies, including Facebook, Amazon, and Google, have relied on private self-certifications schemes, such as Privacy Shield, to assure the EU of "essentially equivalent" protection for personal data of EU residents, despite the extensive scope of U.S. surveillance programs. The U.S. government maintains that the protection under its national security laws "meets" and "exceeds" the safeguards "in foreign jurisdictions, including Europe," suggesting that structural changes in the U.S. legal system are unlikely. Instead, the European Commission ("EC") and U.S. Department of Commerce may soon carve out another solution for EU companies to "contract out" the protection for human rights where public authorities are unwilling to ensure it.

INTERNATIONAL DATA TRANSFERS AND U.S. SURVEILLANCE LAW: *SCHREMS I*

Following the Edward Snowden revelations about mass surveillance programs in 2013, various privacy advocates in the EU opposed the exposure of their personal data to such regimes. Snowden revealed U.S. surveillance programs including PRISIM and UPSTREAM, which collect data directly from undersea cables or from providers. These programs were

authorized by executive powers under the U.S. legal system and often failed to guarantee the basic constitutional rights for U.S. citizens, let alone foreigners. The long-running Schrems saga began when Austrian privacy activist, Maximillian Schrems, lodged one such complaint with the Irish Data Protection Commissioner ("DPC") about Facebook Ireland's transfer of data to the United States. His complaint highlighted the incompatibility of U.S. surveillance programs and existing EU law permitting transfers to the United States. Under EU law at the time, the EC's Safe Harbor Decision created an arrangement where U.S. data importers could "self-certify" that they provided "essentially equivalent" to that guaranteed under EU law, including the protection of fundamental rights under the EU Charter of Fundamental Rights ("EUCFR"). Schrems challenged the adequacy of these arrangements in ensuring "essentially equivalent" protection in his complaint, which the DPC rejected. Schrems then took his complaint to the High Court of Ireland, which referred two questions to the CJEU in the case now known as *Schrems I*. In that case, the CJEU invalidated Safe Harbor, because it did not afford "essentially equivalent" protection for personal data to that guaranteed under EU law (¶¶ 98, 104–106).

Facebook and other companies then relied upon SCCs, a mechanism created under another EC adequacy decision ("SCC Decision"), which enabled data transfers where contractual arrangements could provide the "essentially equivalent" protection to that under the EU legal order. In 2015, the Irish DPC asked Schrems to reformulate his original complaint in light of the invalidation of Safe Harbor. The revised complaint focused on Facebook's data transfers outside of the EU based on SCCs (*Schrems II* ¶¶ 151–153), claiming the reliance on SCCs could not be valid due to U.S. law obliging private companies to provide access to personal data to public authorities under U.S. surveillance programs. Following the reformulation of his complaint, the EC and U.S. officials replaced Safe Harbor with a new version of a "self-certification" regime for EU-United States data transfers—the EU-United States Privacy Shield.

Based on Schrems' revised complaint, the DPC raised a number of questions before the High Court of Ireland, which then referred 11 questions to the CJEU in *Schrems II*. These questions turned the focus towards the suitability and validity of SCCs and, by inference, the validity of Privacy Shield under the *General Data Protection Regulation* ("*GDPR*").

INTERNATIONAL DATA TRANSFERS CONTINUED: *SCHREMS II*

The *Schrems II* judgement challenges the mechanisms for EU-United States personal data transfers based on fundamental inadequacy of U.S. law to ensure the "essentially equivalent" protection to that guaranteed by EU law. The CJEU found that in circumstances where adequate safeguards exist in third countries, or where contractual terms can provide the "essentially equivalent" protection to EU law, the use of SCCs is valid. The Court then chose to engage directly with the validity of EU-United States data transfers under Privacy Shield, finding it invalid due to the fundamental inadequacy of safeguards for personal data provided by U.S. law.

The CJEU first focused on the standard contractual clauses, finding the SCC Decision valid (¶ 105). However, the Court stressed that data controllers must assess the level of protection afforded across the agreed contractual clauses between the data controller and the third country importer/processor, any access by public authorities to the data, and the legal system of the third country (¶¶ 93, 105). The CJEU reiterated that the SCCs must afford appropriate safeguards, enforceable rights, and effective legal remedies (¶ 103), with data controllers/exporters obliged to act if there is a conflict between the SCCs and third country laws, including an incompatibility with national security laws, by suspending data flows (¶¶ 134–135). Where SCCs cannot provide an "essential equivalent" to EU law, and data controllers have not acted, the CJEU held that National Data Protection Authorities ("DPAs") must suspend, limit, or even ban international data transfers (¶¶ 113, 121).

However, the CJEU held that DPAs cannot act to suspend, limit, or ban data transfers where there is an adequacy decision, such as Privacy Shield, in place. The Court asserted that DPAs "cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection" (¶ 118). The CJEU noted that DPAs must still investigate complaints received, and if concerned about the equivalence of protection under an adequacy decision, bring an action before national courts questioning adequacy. If the national court agrees, it can make reference for a preliminary ruling on the validity of an adequacy decision in question (¶¶ 120, 121).

The CJEU then moved on to assess the adequacy of protection under U.S. law to determine the validity of the Privacy Shield. The Court held it invalid because of the largely unrestrained surveillance regime, a lack of redress under those regimes, and the lack of independence for the ombudsperson (¶ 199). Noting the EC can only make a decision on adequacy if the third country's legislation provides all the necessary guarantees to ensure an adequate level of protection (¶¶ 129, 162, 167), the CJEU assessed the level of protection afforded by the United States. It found that U.S. surveillance regimes like PRISM and UPSTREAM which collect data directly from undersea cables or from providers like Google and Facebook, permitted under section 702 of the Foreign Intelligence Surveillance Act ("section 702 FISA"), were not limited to what was strictly necessary for the purposes of foreign intelligence. In particular, the legislation did not lay down any limitations or scope of the programs nor impose any minimum safeguards (¶¶ 179, 180). The CJEU also assessed the Presidential Policy Directive 28 ("PPD-28"—a response to the Snowden revelations attempting to restrain mass surveillance) and Executive Order 12333 ("EO-12333"—a 1981 order permitting expanded surveillance powers authorized by the executive), finding they did not grant actionable rights against U.S. authorities (¶¶ 181, 182, 184). The CJEU noted that the EU legal order provides a right to a hearing before an independent and impartial tribunal (article 47 of the EUCFR) (¶ 186), and that Privacy Shield created a specific role of an ombudsperson for EU data transfers. However, the Court held that surveillance programs based on section 702 FISA and EO-12333, even when read in conjunction with PPD-28, do not provide data subjects with actionable rights, leaving them with no effective remedy (¶ 192). The CJEU also highlighted a lack of independence in the oversight systems of Privacy Shield, as the role of the ombudsperson was related to the executive (¶ 195). Thus, the Court concluded that the Privacy Shield Decision could not provide an "essentially equivalent" protection for personal data to that guaranteed under the EU legal order and, therefore, was invalid (¶ 199).

SO HOW CAN DATA BE TRANSFERRED TO THE UNITED STATES NOW?

After this pronouncement, many are asking how can data be lawfully transferred from the EU to the United States? The SCCs (and for that matter Binding Corporate Rules) are also unusable because the CJEU in

Schrems II ruled that U.S. law—as a whole—does not provide adequate protection required under EU law for international data transfers. The Court partially answered this question: "transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR." (¶ 202). In other words, the Court has not prohibited data transfers to the United States where "essentially equivalent" safeguards are provided. However, data controllers and exporters now face the very real dilemma of having to contract for the impossible—to form contracts under SCCs or article 46 of the GDPR, which protect the rights of the data subject despite the scope of the U.S. surveillance programs. With the CJEU's findings that because of the extensive U.S. surveillance regime, the United States does not afford essentially equivalent safeguards, and confirmation that SCCs cannot bind a public authority in the third country (¶¶ 123, 125), it now appears impossible to transfer data lawfully from the EU to the United States. Some commentators suggest that not all organizations are subject to the U.S. surveillance regime. However, given the scope of the surveillance programs, as discussed by the CJEU, and the possibility of surveillance access even before the data reaches the data importer, such as through the "tapping" of undersea cables (¶¶ 62–63), the adequacy of protection from surveillance by any company is doubtful.

WILL "CONTRACTING OUT" HUMAN RIGHTS TO THE UNITED STATES BE POSSIBLE?

In light of the fundamental inadequacy of U.S. surveillance law to guarantee the level protection required by EU law, the remaining avenue for data transfers points to the use of contracts under the SCC Decision. Contractual obligations between businesses can play a role in protecting human rights in international law, for example in ensuring workers are protected in supply chains and offshore manufacturing. However, these contracts do not bind the government or public authorities in foreign countries, and the local laws in those countries may still over-ride contractual terms. Therefore, contractual clauses to protect data transferred to the United States will not be adequate because of the extensive surveillance powers granted to public authorities under the U.S. legal system, which can easily override those clauses.

The U.S. surveillance regime shows no sign of contracting. Often, as the CJEU found, there is little specific legislation which limits foreign surveillance programs, instead, they are authorized by a supervisory body or through executive order. While the EU Parliament called to overhaul the U.S. foreign surveillance regime following the Snowden revelations, calls for amendment in the United States were reinvigorated in late 2019 following reported breaches of section 702 FISA. However, proposed reforms have now stalled. With U.S. comments in response to *Schrems II* that the U.S. safeguards for data protection under national security programs "meets" or "exceeds" those in European jurisdictions, the stalemate between the EU and the United States is set to continue.

The use of SCCs in light of the scope of the U.S. surveillance framework places an impossible burden on data controllers to attempt to "contract out" the protection of human rights. The Berlin DPC has already issued advice to data controllers to *cease* EU-United States transfers, reinforcing the importance of a valid legal basis for data transfers. Fines for breaching the GDPR can be up to four percent of a company's global revenue. The CJEU was clear that the DPAs are obliged to act against unlawful transfers, so it seems a risky business for private companies to keep doing "business as usual" after *Schrems II*. "Contracting out" human rights protection will simply not work for the CJEU, where the local laws in third countries, such as the United States, fundamentally violate those rights.

CONCLUSION

Schrems II has lived up to the hype—the decision will have far reaching effects. In response to the judgement, the EC could act quick to negotiate another agreement with the U.S. counterparts, just like it did earlier with the Safe Harbor and Privacy Shield, again authorizing data flows to the United States. However, without changes in the U.S. surveillance regime, we can be certain that any future adequacy decisions will be challenged by privacy advocates, costing DPAs millions of Euros in further court costs. Similarly, attempts to "contract out" human rights protection under SCCs, given the inability of the United States to provide "essentially equivalent" protection, expose data controllers to fines under the GDPR. Yet, the high stakes of the transatlantic economy weaken the EU position, while the bargaining power of the United States suggests that structural changes—that would

bring the United States in line with "essential equivalence"—are unlikely any time soon. Failing U.S. changes, tech companies might have to process personal data in Europe, as legally "contracting out" protection for human rights might be next to impossible.