REJECTING THE TRANSATLANTIC OUTSOURCING OF DATA PROTECTION IN THE FACE OF UNRESTRAINED SURVEILLANCE

MONIKA ZALNIERIUTE AND GENNA CHURCHES

(2021) 80(1) *Cambridge Law Journal*, 8
[2021] *UNSWLRS* 32

UNSW Law
UNSW Sydney NSW 2052 Australia

M. Zalnieriute and G. Churches, 'Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance' *Cambridge Law Journal*, 80(1), 2021, pp. 8-11

REJECTING THE TRANSATLANTIC OUTSOURCING OF DATA PROTECTION IN THE FACE OF UNRESTRAINED SURVEILLANCE

MONIKA ZALNIERIUTE[1] AND GENNA CHURCHES[2]

Abstract

On 16 July 2020, the Grand Chamber of the Court of Justice of the European Union ('CJEU'), in a departure from the Advocate General's ('AG') Opinion, invalidated the the key mechanism for EU-United States data transfers, Privacy Shield for not affording 'essentially equivalent' protection to that provided under the EU legal order for personal data transferred to the US. The Court upheld the validity of the SCC for international data transfers, ruling that the National Data Protection Authorities ('DPAs') must take action where these clauses do not provide 'essentially equivalent' protection to EU law. The *Schrems II* judgement will have significant implications for many areas of EU law and policy, transatlantic relations and global data governance more generally. It will impact the EU-US data transfers, data transfers to third countries beyond US, including the post-Brexit UK, because SCCs are relied on by 88 per cent of EU companies transferring data outside the EU. Following the Snowden revelations in 2013, the CJEU has developed a powerful body of jurisprudence which rejects the transatlantic outsourcing of data protection without adequate safeguards. *Schrems II* reasserted the fundamental role of data protection in the EU legal order and transatlantic relations, and emphasised the need for EU to suspend, limit, or even block data transfers to countries where fundamental rights are not protected. Full implications of *Schrems II* are yet to be seen but the effects will be felt for many years to come.

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

[1] Senior Lecturer, Faculty of Law & Justice, UNSW Sydney; Leader of 'AI and Law' research stream, Allens Hub for Technology, Law and Innovation; Australian Research Council Discovery Early Career Research Award Fellow (project number DE210101183), m.zalnieriute@unsw.edu.au.

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

In Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ('*Schrems II*') (EU:C:2020:559) the EU judicature was requested by the High Court of Ireland, to ascertain the validity of the Standard Contractual Clauses Decision (2010/87/EU OJ L 39, p. 5–18 'SCC Decision') and, by inference, the Privacy Shield Decision (2016/1250/EU OJ L 207, p. 1–112 'Privacy Shield') for transfers of personal data by Facebook from the EU to the US under the Data Protection Directive 95/46/EC ('DPD') (OJ 1995 L 281/31) replaced by General Data Protection Regulation ('GDPR') 2016/679 (OJ 2016 L 119/1) and primary EU law, particularly provisions relating to respect for private life and the protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights ('EUCFR').

On 16 July 2020, the Grand Chamber of the Court of Justice of the European Union ('CJEU'), in a departure from the Advocate General's ('AG') Opinion (EU:C:2019:1145), invalidated the Privacy Shield for not affording 'essentially equivalent' protection to that provided under the EU legal order for personal data transferred to the US. The Court upheld the validity of the SCC for international data transfers, ruling that the National Data Protection Authorities ('DPAs') must take action where these clauses do not provide 'essentially equivalent' protection to EU law. *Schrems II* is the second decision stemming from the long running challenge of Facebook Ireland's transfers of personal data to the US by privacy activist Maximillian Schrems. Following the Snowden revelations about mass surveillance programmes in 2013, Schrems lodged a complaint with the Irish Data Protection Commissioner ('DPC'), challenging the adequacy of safeguards under the 'Safe Harbour' arrangements which had authorised EU-US data transfers since 2000 (OJ L 215, 25/08/2000 p.7-47 'Safe Harbour'). After the DPC rejected his complaint, Schrems took the matter to the High Court of Ireland, which then referred to the CJEU. In 2015, the Grand Chamber of the CJEU invalidated Safe Harbour for not ensuring 'essentially equivalent' protection for personal data transferred to the US, as required by Article 25(6) DPD, read in the light of EUCFR (*Maximillian Schrems v Data Protection Commissioner* C-362/14, EU:C:2015:650, at: [96]-[98], [103]-[106]).

After the invalidation of Safe Harbour, the Irish High Court referred Schrems' complaint back to the DPC for assessment, who then requested Schrems reformulate his original complaint. Schrems's reformulated complaint challenged Facebook's data transfers to the US based on SCC's, which, Schrems claimed, could

not be valid because private companies must provide US national security agencies with access to data transferred from the EU. Doubting the adequacy of safeguards provided under the SCC Decision, the DPC requested a determination from the High Court. The High Court examined the US regime, and, sharing doubts on the validity of the SCC Decision, referred 11 questions to the CJEU, primarily focused on the validity of the SCC Decision and actions DPAs can take. *Schrems II,* therefore, presented the CJEU with another opportunity to articulate data protection requirements for international data transfers.

AG Saugmandsgaard Øe's Opinion (EU:C:2019:1145) recommended that the CJEU find the SCC Decision valid as SCCs are a general mechanism for transfers (at: [120]), however, he advised that the Court does not need not engage with questions on the validity of Privacy Shield (at: [161]-[166], [187]) as; the CJEU was not specifically asked by the High Court (at: [179]), and a direct challenge on the validity of Privacy Shield was underway in the General Court (at: [179]) see (*Quadrature du Net*, Case T-738/16).

In delivering its judgement, the Grand Chamber of the CJEU first determined that SCCs can be validly used under Article 46(1) GDPR. The Court outlined the responsibility to suspend, or ban data international data transfers where SCCs do not provide 'essentially equivalent' protections to EU law (at: [103]). The Court affirmed data controllers have an obligation to suspend data flows where the SCC terms conflict with local laws in the third countries (at: [134]-[135]). However, because SCCs cannot alter local laws or bind public authorities, the CJEU found data controllers must not contract to export data to countries with incompatible national security laws, and must freeze data flows if local laws change or the importer fails to follow SCCs (at: [105], [93]). While data controllers *are* the first layer of protection in this process, the Court held the DPAs *must* act on complaints where data transfers under SCCs do not afford 'essentially equivalent' protection to EU law (at: [113], [121])

The CJEU then departed from the AG's Opinion, addressing the validity of Privacy Shield. It noted the European Commission could only make an adequacy decision if 'the third country's relevant legislation' provides 'all the necessary guarantees' to conclude that the 'legislation ensures an adequate level of protection' (at: [129]). The Court then assessed whether the US provided that level of protection. The Court first examined the US Foreign Intelligence Surveillance Act ('s 702'), which regulates

programmes tapping undersea cables such as PRISM, finding it failed to satisfy the principle of proportionality as it lacked 'clear and precise rules governing the scope and application' of the measures in question (at: [179], [180]). The CJEU then considered Presidential Policy Directive 28 ('PPD-28'), a reform attempting to restrain mass surveillance, which, it found, does not provide effective and enforceable rights (at: [181]). Similarly, the Executive Order 12333('EO'), from 1981 authorising expanded surveillance powers by the executive, also failed to provide enforceable rights against US authorities (at: [182]).

The Court then noted the EU legal order provides a right to a hearing before an independent and impartial tribunal (Article 47 EUCFR) (at: [186]). In this regard, the Court found that the appointment and/or dismissal of the ombudsperson under Privacy Shield was not sufficiently independent from the executive (at: [195]). Further, surveillance programs based on s 702 and EO, even when read in conjunction with PPD–28 did not provide data subjects with actionable rights, leaving no effective remedy against US authorities (at: [192]). Therefore, the CJEU concluded that the Privacy Shield does not provide 'essentially equivalent' protection to EU laws and was invalid (at: [199]-[201]).

The *Schrems II* judgement will have significant implications for many areas of EU law and policy, transatlantic relations and global data governance more generally. First, the CJEU's pronouncement impacts EU-US data transfers. A ruling that US laws do not provide 'essentially equivalent' protection and the invalidation of Privacy Shield, puts the legality of commercial transfers of personal data from the EU to the US in doubt. Although the Court did not invalidate the SCC Decision, using SCCs to ensure the 'essentially equivalent' protection for data transferred to the US is difficult because the CJEU ruled that US does not provide the necessary safeguards. Companies may have no alternative but to process data within the EU or await a further decision on adequacy from the EC. Another mechanism under EU law — Binding Corporate Rules — might offer an alternative mechanism for data transfers to US. However, the Court recognised Irish High Court findings that undersea cable tapping may expose EU personal data to surveillance well before it reaches its US destination (at: [62]-[63]). Thus, any contractual terms outsourcing the protection of personal data to US, would be invalid due to the scope of the US surveillance programmes. The US Government commented that it already provides an equivalent protection to EU law, denoting structural reform in the US is unlikely in the near future. A more likely

outcome will be another *Quick* '*Harbour*' or '*Shield*' accommodating the US institutional preferences. Such outsourcing of personal data protection in the face of unrestrained surveillance would set the stage for *Schrems III*.

Second, *Schrems II* will have significant implications for data transfers to third countries beyond US, including the post-Brexit UK, because SCCs are relied on by 88 per cent of EU companies transferring data outside the EU. While data transfers using SCC were upheld, *Schrems II* has put data controllers on notice — they must make assessments before exporting data to third countries and monitor those arrangements, suspending data flows if needed. The CJEU also made it clear that the DPAs must use their regulatory and investigative powers confidently, adopting corrective measures where data controllers fail to act or make agreements using SCCs which do not afford 'essentially equivalent protection', and challenging European Commission adequacy decisions where DPAs doubt the adequacy of third country safeguards.

Following the Snowden revelations in 2013, the CJEU has developed a powerful body of jurisprudence which rejects the transatlantic outsourcing of data protection without adequate safeguards. *Schrems II* reasserted the fundamental role of data protection in the EU legal order and transatlantic relations, and emphasised the need for EU to suspend, limit, or even block data transfers to countries where fundamental rights are not protected. Full implications of *Schrems II* are yet to be seen but the effects will be felt for many years to come.