British Institute of International and Comparative Law

ASSESSING THE IMPLICATIONS OF *SCHREMS II* FOR EU–US DATA FLOW

MARIA HELEN MURPHY*

Abstract With the constant flow of data across jurisdictions, issues regarding conflicting laws and the protection of rights arise. This article considers the EU–US data transfer relationship in the aftermath of the decision in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* where the Court of Justice of the European Union (CJEU) invalidated an EU–US data transfer agreement for the second time in just five years. This judgment continues the line of cases emphasising the high value the Court places on securing EU personal data in accordance with EU data protection standards and fundamental rights. This article assesses the implications of the ruling for the vulnerable EU–US data transfer relationship.

Keywords: EU law, General Data Protection Regulation, Privacy Shield, adequacy, Standard Contractual Clauses, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*.

I. INTRODUCTION

The European Union model of data protection regulation has been remarkably influential on laws and practices adopted worldwide. Due to the instrumental role personal data plays in the operation of the modern economy and society, the importance and potential implications of this influence are difficult to overstate. Not only has the EU impacted the development of data protection laws globally, but it has also 'taken an essential role in shaping how the world thinks about data privacy'.[1]

A core premise of EU data protection law is that personal information can only be transferred outside of the EU to the jurisdiction of a 'third country' under certain conditions. This is logical as it would defeat the purpose of data protection law if data could be processed without any restriction as soon as it

* Associate Professor in Law, Maynooth University, maria.murphy@mu.ie.

[1] P Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYULR 771, 773. For examples of early acceptance of similar principles in the USA, Europe, Australia, New Zealand, Japan, and Canada, see L Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014) 108–9.

[*ICLQ* vol 71, January 2022 pp 245–262] doi:10.1017/S0020589321000348

flowed out of the EU.[2] The General Data Protection Regulation (GDPR)—and the Data Protection Directive before it[3]—sets out a number of ways by which transfers can be facilitated. For example, data can be transferred to a third country on the basis of an 'adequacy decision' where the Commission has determined that the third country ensures an 'adequate level of protection' for personal data.[4] The EU, as represented by the Commission, has sought compromise in its data transfer negotiations with the US—as evidenced by both the Safe Harbour and Privacy Shield agreements discussed further below. The impetus to reach compromise can be explained by the fact that transfers of personal data between the EU and the US are an integral element of the transatlantic commercial relationship.[5]

Indeed, the significance of the EU–US data transfer relationship is unparalleled, in large part due to the dominance of US technology companies and the size of the EU consumer market. In spite of its importance to both parties, tensions have arisen in the relationship over the years. For example, following the achievement of compromise with the Safe Harbour Agreement in 2000,[6] the newly established Bush Administration took issue with the extraterritorial application of the 'burdensome' EU standards.[7] The EU efforts were branded as protectionist and contrary to the 'worldwide trend for global trade liberalization.'[8] In one Congressman's criticism, the Data Protection Directive was described as having the potential to become the 'de-facto privacy standard on the world'.[9] While attitudes have shifted over time and US companies now generally accept their obligation to take heed of EU data protection standards, opposition remains in some quarters.[10]

[2] And Norway, Liechtenstein, and Iceland.

[3] European Parliament and Council Directive (EC) 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, art 25.

[4] European Parliament and Council Regulation (EU) 2016/679 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 [2016] OJ L119/1 (GDPR) art 45.

[5] Communication from the Commission to the European Parliament and the Council, 'Rebuilding Trust in EU-US Data Flows' COM(2013) 846 final, 2.

[6] Commission Decision (EC) 2000/520 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 (notified under document number C(2000) 2441) (Text with EEA relevance.) [2000] OJ L215/7, 14.

[7] C Arthur, 'Now Bush Wants to Scrap Deal on Internet Privacy' *The Independent* (London, 31 March 2001) 11.

[8] M Huie, S Laribee and S Hogan, 'The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues' (2002) 9 Tulsa Journal of Comparative and International Law 391, 401.

[9] House Of Representatives, 'The EU Data Protection Directive: Implications For The US Privacy Debate: Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce' (8 March 2001) Serial No 107-19 <https://www.govinfo.gov/content/pkg/CHRG-107hhrg71497/html/CHRG-107hhrg71497.htm>.

[10] See, for example, W Ross, 'EU Data Privacy Laws are Likely to Create Barriers to Trade' *Financial Times* (London, 30 May 2018) <https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c>.

In spite of continued criticisms of both systems and their interactions under the Safe Harbour agreement, the jurisdictions had settled into a somewhat uneasy truce where an imperfect system of protection remained in place on a pragmatic basis in order to facilitate data transfers and free trade. It is important to note that subsequent to the adoption of the Safe Harbour Agreement in 2000, EU data protection law has continued to strengthen. With the entering into force of the Lisbon Treaty giving binding status to the Charter of Fundamental Rights (CFR)[11] and the passage of the GDPR, the EU has continued on a trajectory of safeguarding the rights to respect for private life and protection of personal data. Impetus was added by the Court of Justice of the European Union (CJEU) which has interpreted the law expansively in pursuit of protecting fundamental rights. A key disrupting event to the prevailing EU–US data transfer agreement occurred in 2013 with the release of documents by Edward Snowden revealing the extent of US government surveillance programmes. The decision of the CJEU in *Digital Rights Ireland*—delivered in the aftermath of the disclosures—made clear that the integration of privately-held data into the US surveillance apparatus presented a particularly thorny challenge to the continuance of the transatlantic data transfer status quo.[12]

The subsequent cases dealing specifically with the EU–US data transfer relationship have demonstrated that the EU Commission model of negotiation with the US is unlikely to withstand the scrutiny of the CJEU without a radical shift in the US approach to surveillance law. In particular, this article examines the EU–US relationship following the ruling in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (*Schrems II*)[13] where the CJEU invalidated an EU–US data transfer agreement for the second time in just five years. The emphasis in the judgment on proportionality and safeguards continues a notable trend in the privacy and data protection jurisprudence and demonstrates the unwillingness of the CJEU to compromise on the matter of fundamental rights for economic expedience. While *Schrems II* is a clear rejection of the status quo by the CJEU, what is to come in its wake remains unsettled. In order to understand the

[11] Charter of Fundamental Rights of the European Union [2000] OJ C364/1 (CFR). Article 7 CFR guarantees the right to respect for private and family life and Article 8 CFR guarantees the right to protection of personal data.

[12] Developments in US case law subsequent to the Snowden revelations should be noted. For example, the US Court of Appeals for the Ninth Circuit found that a now discontinued programme of bulk collection of telephone metadata violated the Foreign Intelligence Surveillance Act, *United States v Moalin* 973 F3d 977 (9th Cir 2020).
While the Ninth Circuit did not decide on the constitutionality of the metadata programme, it is notable that the Court cited the Supreme Court case of *Carpenter v United States* in deciding that the third-party doctrine did not apply due to the scale and comprehensiveness of information collected through the programme, *Carpenter v United States* 585 US (2018). See also MH Murphy, *Surveillance and the Law: Language, Power, and Privacy* (Routledge 2019) 26–32.

[13] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* EU:C:2020:559.

implications of the decision, it is necessary to consider the key cases that preceded it.

II. FROM *DIGITAL RIGHTS IRELAND* TO *SCHREMS I* AND *SCHREMS II*

The 2014 ruling of the CJEU in *Digital Rights Ireland* demonstrated the commitment of the CJEU to upholding the rights to respect for private life and the protection of personal data as guaranteed by the CFR in the face of ever-increasing data collection. It was the first opportunity for the Court to address these issues in the wake of the Snowden revelations. In *Digital Rights Ireland*, the CJEU considered the Data Retention Directive, which had mandated that Member States compel the retention of all communications metadata for between six and 24 months.[14] After finding that the general application of the Directive constituted a disproportionate interference with Articles 7 and 8 CFR,[15] the CJEU found the Directive to be invalid.[16] Within its clear rebuke of generalised surveillance programmes, an additional preview of the future direction of the case law can be found in paragraph 68 where the CJEU states:

> it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a

[14] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] OJ L105/54.

[15] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* EU:C:2014:238, para 69.

[16] ibid paras 38 and 46; Directive 2006/24/EC (n 14). It should be noted that the landmark decision in *Digital Rights Ireland* draws from the extensive surveillance case law of the European Court of Human Rights (see also Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others* EU:C:2003:294, para 75). The ruling in *Digital Rights Ireland* goes further than prior ECtHR case law by recognising that indiscriminate and generalised data collection is a 'particularly serious' interference with private life, Joined Cases C-293/12 and C-594/12 (n 15) para 39. Notably, the ECtHR has subsequently been influenced by developments at the CJEU. In *Szabó and Vissy v Hungary*, the ECtHR cites *Digital Rights Ireland* and the *Schrems I* case (Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650, discussed below) and recognises the contribution the CJEU has made in 'redefining the limits of covert data gathering for national security purposes in the EU and outside it' *Szabó and Vissy v Hungary* [2016] ECHR 579, 15–16. While differences persist between the approaches of the Courts, cross-referencing has continued. For example, in *Tele2 Sverige*, the CJEU cited more recent ECtHR case law including the aforementioned *Szabó and Vissy v Hungary* and *Roman Zakharov v Russia* [2015] ECHR 1065, see Case C-203/15 *Tele2 Sverige v Post-och telestyrelsen* EU:C:2016:970, paras 119–20. See also citations by the ECtHR in *Big Brother Watch v United Kingdom* [2021] ECHR 439. MH Murphy, 'Algorithmic Surveillance: The Collection Conundrum' (2017) 31(2) IRLCT 225.

> control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[17]

In spite of the decision in *Digital Rights Ireland* being focused on the disproportionality of EU data retention legislation, it was clear that this particular statement would have 'significant implications for multinationals that move information between the EU and other states'.[18] The fact that the Snowden disclosures revealed the capability of the US intelligence agencies to access user information held by US technology companies is likely to have influenced the strong position taken by the CJEU on the matter.[19] The emphasis placed on the role of an independent authority as explicitly provided for in the Charter is also notable and foreshadows developments in subsequent case law.[20]

As previously mentioned, the Commission is empowered to make adequacy decisions determining that a third country provides an 'adequate level of protection' for personal data. Such a decision enables the free flow of information between the EU and the third country and this brings significant economic benefits. Before making such a decision, the Commission is required to take into account certain factors when determining whether adequate protection is provided. In particular, the Commission is required to take account of 'the rule of law, respect for human rights and fundamental freedoms', relevant domestic legislation and its implementation, and the 'existence and effective functioning of one or more independent supervisory authorities'.[21] As this sets a high bar for third countries, there are other mechanisms that allow for the transfer of personal data out of the EU where the data exporter has provided appropriate safeguards and where data subjects have enforceable rights and effective legal remedies.[22]

The more prominent mechanisms through which such transfer can be lawfully achieved are 'standard contractual clauses'[23] (SCC) and 'binding corporate rules' (BCR).[24] BCR are designed to facilitate data transfers within an organisation and must be approved by the competent domestic supervisory authority in accordance with Article 63 of the GDPR.[25] The most popular tool for third-country data transfers is reported to be SCC which allow organisations to transfer personal data to third countries on the basis of European Commission-approved model data protection clauses.[26] In order to rely on SCC, data exporters must include the data protection clauses in their contracts with relevant data importers in order to impose legal obligations on both parties. As an alternative to these mechanisms, it may be possible to

[17] Joined Cases C-293/12 and C-594/12 (n 15) para 68.
[18] MH Murphy, 'The Pendulum Effect: Comparisons between the Snowden Revelations and the Church Committee. What Are the Potential Implications for Europe?' (2014) 23 ICTL 192, 210.
[19] ibid.
[20] Joined Cases C-293/12 and C-594/12 (n 15) para 68.
[21] GDPR (n 4) art 45(2).
[22] ibid art 46.
[23] ibid art 46(2)(d).
[24] ibid arts 46(2)(b), 47.
[25] ibid art 47.
[26] ibid arts 46(2)(c) and 93(2).

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

transfer data due to the application of a derogation in certain limited circumstances.[27] For example, a transfer may be possible where a 'data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers' or where 'the transfer is necessary for the performance of a contract between the data subject and the controller'.[28]

Even though an adequacy decision has been seen as the gold standard enabling free-flowing data transfer between the EU and third countries,[29] the United States has never sought a full adequacy determination from the EU Commission—reportedly because it did not expect to achieve one.[30] While US companies have always had the option to utilise other transfer mechanisms, they were generally viewed as 'relatively costly and inflexible' alternatives to an adequacy finding.[31] In light of this, the European Commission and the US have engaged in bilateral negotiations in order to create sui generis instruments designed to facilitate the streamlined transfer of data from Europe to the US. The first programme agreed, as previously mentioned, was dubbed the Safe Harbour Agreement and operated from 2000 to 2015. The legal basis for the Safe Harbour arrangement was provided in the Commission Decision 2000/520/EC.[32] Under the Safe Harbour Agreement, US-based companies were able to voluntarily self-certify as being compliant with the Safe Harbour principles of (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement. The Safe Harbour programme achieved significant adoption and is credited with familiarising US privacy practitioners with EU data protection standards and bringing EU norms into the mainstream of global discussions about privacy regulation.[33]

The Safe Harbour Agreement was at the centre of the ruling in *Schrems I* where Mr Schrems had challenged the refusal of the Irish Data Protection Commissioner (DPC) to investigate his complaint against Facebook Ireland. Mr Schrems argued that Facebook transfers of personal data to the US were incompatible with European data protection law. The DPC had refused to investigate the matter on the grounds that the adequacy finding of the Commission, as formalised in the Safe Harbour Decision, permitted the transatlantic transfers and that it was not the role of the Irish supervisory

[27] See ibid art 49. [28] ibid art 49(1)(a).

[29] The certainty of adequacy determinations seems under threat, however, based on recent case law and the fact that the Commission is continually reviewing existing adequacy decisions. 'EU Commission's Review of Existing Adequacy Decisions Well Underway' (*Privacy Laws*, 3 July 2019) <https://www.privacylaws.com/news/eu-commission-s-review-of-existing-adequacy-decisions-well-underway/>.

[30] C Wolf, 'Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers' (2013) 43 WUJL&P 227, 229.

[31] Schwartz (n 1) 794.

[32] Commission Decision (EC) 2000/520 (n 6) 14; Case C-362/14 (n 16) para 2.

[33] Schwartz (n 1) 799.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

authority to question the Commission's Decision. Mr Schrems challenged this position in the Irish High Court. Before referring its questions to the CJEU, the Irish High Court referred to US surveillance practices noting that the 'accuracy of much of the Snowden revelations does not appear to be in dispute'.[34] In the subsequent Opinion of Advocate General Bot, it was remarked that the revelations 'brought to light the existence of large-scale information-gathering programmes in the United States' and gave rise to 'serious concerns as to whether the requirements of EU law are observed when personal data is transferred to undertakings established in the United States'.[35] Of particular relevance to Facebook was Section 702 of the Foreign Intelligence Surveillance Act which has been used to authorise non-targeted surveillance programs (such as PRISM) on the basis of annual certifications.[36]

Having confirmed that the existence of a Commission adequacy decision does not exempt a supervisory authority from investigating a complaint in regard to third country transfers of personal data, the Grand Chamber of the CJEU went on to consider the validity of the Safe Harbour Decision.[37] The Court found that when assessing whether the data protection regime of a third country meets the requirements for adequacy, the level of protection required should be 'essentially equivalent' rather than 'identical' to the level of protection guaranteed within the EU.[38] Without such a requirement, the high standards of protection required by the EU would be undermined and open to circumvention by transfers of personal data to third countries for the purpose of being processed in those countries.[39] The CJEU did not engage in a substantive analysis of whether the principles set out in the Safe Harbour Agreement ensured an adequate level of protection.[40] Instead, the CJEU placed emphasis on the requirement to 'take account of all the circumstances surrounding a transfer of personal data to a third country' including circumstances that have arisen—or been brought to light—subsequent to when the data transfer agreement was reached.[41] Crucially, increased understanding of the scope of US surveillance programmes had emerged following the Snowden disclosures.

The Court pointed out that as Safe Harbour relied on a voluntary system of self-certification that 'effective detection and supervision mechanisms' were necessary to ensure effectiveness.[42] A key issue found with the Safe Harbour Decision was the provision limiting the application of the Safe Harbour principles 'to the extent necessary to meet national security, public interest,

[34] See Case C-362/14 (n 16) para 36; *Schrems v Data Protection Commissioner* [2014] IEHC 310 [13].

[35] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:627, Opinion of Advocate General Bot, paras 4 and 237.

[36] Case C-362/14 (n 16) para 22.

[37] ibid paras 61–2. The Court retains sole jurisdiction to declare an EU act to be invalid.

[38] ibid para 73.

[39] ibid paras 72–3.

[40] The CJEU highlighted that Decision 2000/520 did not state that the United States 'ensures' an adequate level of protection and that as a result there was no need to examine the content of the Safe Harbour principles (ibid paras 97–8).

[41] ibid paras 75–7.

[42] ibid para 81.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

or law enforcement requirements'.[43] The Court found that the general nature of this derogation enabled interference with the fundamental rights of persons whose personal data was transferred from the EU to the US on very broad grounds.[44] The CJEU criticised the absence of objective criteria to be used to determine the limits of public authority access and use for purposes which are 'specific, strictly restricted and capable of justifying the interference'.[45] The Court went so far as to state that:

> legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[46]

The absence of the rule of law safeguard and fundamental right of effective judicial protection[47] was also strongly criticised.[48]

In spite of the decision in *Schrems I* being foreshadowed in *Digital Rights Ireland*, it sent shock waves through entire industries dependent on transatlantic data transfers. Due to the complexity of the arrangements, the European Supervisory Authorities agreed to give time to companies needing to transition from the Safe Harbour mechanism in the immediate aftermath of the ruling.[49] The value placed on the transatlantic relationship was clear by the prompt entering into negotiations between the EU Commission and the US Department of Commerce in order to develop a new agreement, to be called the Privacy Shield.[50] With the European Parliament providing final approval in July 2016, the agreement was officially in place from August 2016.[51] While the seven Privacy Shield Principles largely aligned with the Safe Harbour principles, additional measures and safeguards were introduced in an effort to respond to the concerns of the CJEU. Of note was the development of the principle of 'Recourse, Enforcement and Liability'.[52]

Another response to the ruling in *Schrems I* was the setting out of some limitations on US Government access to data in letters from official sources.

[43] ibid para 84. [44] ibid para 87. [45] ibid para 93. [46] ibid para 94.
[47] CFR (n 11) art 47. [48] Case C-362/14 (n 16) para 95.
[49] S Monteleone and L Puccio, *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules* (European Parliamentary Research Service 2017).
[50] Although negotiations to improve the Safe Harbour agreement had already been commenced. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ L207/1; see 'EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield, Press Release' (*European Commission*, 2 February 2016) <http://europa.eu/rapid/press-release_IP-16-216_en.htm>.
[51] 'European Commission launches EU-US Privacy Shield: Stronger Protection for Transatlantic Data Flows' (*European Commission*, 12 July 2016) <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461>.
[52] 'Privacy Shield Framework: 7. Recourse, Enforcement And Liability' (*Privacy Shield*) <https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY>.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

The letter from the US Secretary of State contains a commitment to establishing a new Privacy Shield Ombudsperson for inquiries relating to US signals intelligence.[53] The letter from the US Department of Justice sets out the safeguards and limitations on US government access for law enforcement and public interest purposes.[54] The letter from the Office of the Director of National Intelligence sets out the safeguards and limitations applicable to US national security authorities and contains assurances that Presidential Policy Directive 28 (PPD-28)[55] would provide privacy protections regardless of nationality.[56] Based on these representations from the US Government, the Commission concluded that US rules limit interference with the fundamental rights of EU data subjects for US national security purposes to what is 'strictly necessary to achieve the legitimate objective in question'.[57] While the new framework was criticised by privacy and data protection advocates as not remedying the core faults identified with Safe Harbour,[58] the 'continuity in basic vocabulary and orientation' offered easy adaptability for US companies and the strengthening of the agreement was seen by some as constituting a development in 'transatlantic data privacy norms'.[59]

Following the outcome in *Schrems I*, the DPC sought to fulfil its obligation to investigate the complaint of Mr Schrems regarding the transfer of personal data by Facebook from the EU to the US.[60] It emerged that Facebook had relied on SCC[61] as opposed to the Safe Harbour Agreement for EU–US transfers and Mr Schrems was asked to reformulate his complaint in light of this.[62] Subsequently, the DPC asked the Irish High Court to make a reference for a preliminary ruling to the CJEU concerning the validity of SCC. This reference resulted in the *Schrems II* judgment, delivered by the Grand Chamber in July 2020. The judgment of the CJEU in *Schrems II* continues the line of cases emphasising the high value the Court places on securing EU

[53] Decision 2016/1250 (n 50) Annex III.

[54] ibid Annex VII.

[55] Issued by President Obama in January 2014.

[56] Decision 2016/1250 (n 50) Annex VI. Kerry and Raul point out how the PPD-28 was a 'keystone underlying support for the Privacy Shield': C Kerry and A Raul, 'The Economic Case for Preserving PPD-28 and Privacy Shield' (*Lawfare*, 17 January 2017) <https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield>.

[57] Decision 2016/1250 (n 50) para 88.

[58] M Schrems, 'Privacy Shield Statement' (Press Breakfast by MEP Jan Albrecht, European Parliament, Brussels, 12 July 2016) <www.europe-v-facebook.org/PA_PS.pdf>; Indeed, the EDPS opined that the Privacy Shield should be considered an 'interim instrument for the short term. Something more robust needs to be conceived': C Stupp, 'EU Privacy Watchdog: Privacy Shield Should Be Temporary' (*EURACTIV*, 3 August 2017) <https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/>.

[59] Schwartz (n 1) 802.

[60] Case C-311/18 (n 13) para 56.

[61] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5 as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 [2016] OJ L344/100 (Commission SCC Decision). A revision process of the Commission SCC Decision is ongoing.

[62] 'EU-US Data Transfers' (*noyb*) <https://noyb.eu/en/project/eu-us-transfers>.

personal data in accordance with EU data protection standards. The two issues of primary concern for the purposes of this article are the findings of the CJEU as regards the validity of SCC and the Privacy Shield.[63]

Beginning with the issue of SCC, the CJEU referred to recital 108 of the GDPR which states that, in the absence of an adequacy decision, the party exporting data to a third country should take measures to compensate for the lack of data protection by providing appropriate safeguards. The safeguards applied—which may be provided through the use of SCC or other mechanisms—should 'ensure compliance with data protection requirements and the rights of data subjects'.[64] In line with transfers made on the basis of an adequacy decision, the safeguards must be capable of ensuring a level of protection 'essentially equivalent' to that guaranteed by EU law read in light of the Charter.[65] In addition to considering the contractual clauses agreed between the data exporter and importer, it is also necessary to consider the legal system of the third country and any potential access to the transferred personal data by public authorities.[66] The need to consider the legal system and potential for public authority access in the third country is highly pertinent to the issue of EU–US data transfers following the Snowden revelations.

As the terms of SCC are only binding on the third-country recipient of the data and not on government authorities, it may be impossible to guarantee the necessary protection of EU data solely on the basis of the SCC, for example where government authorities have unfettered access to data.[67] Instead of declaring the use of SCC to be invalid in such circumstances, the CJEU recommends the adoption of supplementary measures in order to ensure compliance with EU standards of protection.[68] The Court makes clear that the data exporter must, on a case-by-case basis, examine the law of the relevant third country and provide additional safeguards where necessary to ensure adequate protection. Transfers of personal data that do not meet the standard should be suspended by the data exporter in the first instance or by the relevant national supervisory authority.[69]

According to the CJEU, the validity of SCC depends on whether effective mechanisms exist to ensure compliance in practice.[70] Where national law compels the sharing of personal data in a manner that goes beyond what is necessary in a democratic society to protect national security, defence, and public security, compliance with such an obligation is a breach of the SCC.[71] The CJEU concluded that the SCC Decision provides for effective mechanisms capable of ensuring that third-country data transfers are stopped where the

[63] Another finding of the CJEU in *Schrems II* was that the GDPR applies to third-country data transfers for commercial purposes even where the data is liable to be processed by government authorities of the third country for the purposes of public security, defence, and State security (Case C-311/18 (n 13) para 80).
[64] ibid para 95.
[65] ibid paras 93, 99, 105.
[66] ibid para 105.
[67] ibid paras 126 and 133.
[68] ibid paras 133–4.
[69] ibid paras 135–7.
[70] ibid para 137.
[71] ibid para 141.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

recipient of the transfer does not comply or is unable to comply with the conditions of the SCC.[72] While this result means that the SCC Decision remains valid, it is difficult to see what safeguards or supplementary measures can be implemented that will rectify the fundamental issues identified with the US intelligence regime.[73] This is discussed further in Section V where the implications of *Schrems II* are considered.

In spite of the DPC only seeking clarity regarding the SCC Decision, the questions referred by the Irish High Court regarding the level of protection required under Articles 7, 8, and 47 of the Charter compelled the CJEU to take into account the changes brought about by the Privacy Shield Decision —including the introduction of an ombudsperson.[74] Accordingly, the CJEU examined whether the Privacy Shield Decision complied with the GDPR read in light of the Charter.[75] Even though the EU Commission found that the Privacy Shield agreement ensured an adequate level of protection for personal data transferred to the US, the CJEU highlighted the fact that the Privacy Shield Decision states that adherence may be limited 'to the extent necessary to meet national security, public interest, or law enforcement requirements'.[76] This enables interference with personal data transferred from the EU to the US through US intelligence programmes.[77]

In its Privacy Shield Decision, the Commission found that such interference 'will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference'.[78] In assessing the Commission's Decision, the CJEU pointed out that the proportionality requirement means that laws which entail such interference must:

> lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing.[79]

In particular, when assessing whether to grant an adequacy determination, the Commission must 'take account of "effective and enforceable data subject rights" for data subjects whose personal data are transferred'.[80]

The CJEU found that the Privacy Shield Decision could not provide a level of protection 'essentially equivalent' to that arising from the Charter.[81] The US

[72] ibid para 148. [73] ibid para 149. [74] ibid paras 151–2. [75] ibid para 161.
[76] ibid paras 163–4. [77] ibid para 165. [78] ibid para 167.
[79] ibid para 176, referencing Opinion 1/15 *Transfer of Passenger Name Record data from the European Union to Canada* EU:C:2017:592, paras 140–1. [80] GDPR (n 4) art 45(2)(a).
[81] Case C-311/18 (n 13) para 181.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

intelligence regime examined by the CJEU confers extremely broad power on US government agencies to engage in unlimited bulk surveillance for the purposes of foreign intelligence.[82] As the legal basis for interferences with fundamental rights must 'lay down clear and precise rules governing the scope and application of the measure in question' and impose minimum safeguards, the US system could not be deemed to meet the standards of proportionality according to the CJEU.[83]

Adequacy determinations must take into account the potential for individuals to seek effective administrative and judicial redress.[84] Moreover, effective independent data protection supervision must exist and provision should be made for cooperation with EU data protection authorities.[85] In the Privacy Shield Decision, the Commission had found that the introduction of the ombudsperson mechanism and role as 'Senior Coordinator for International Information Technology Diplomacy'[86] brought the protection provided by the Privacy Shield agreement to a level 'essentially equivalent to that guaranteed by Article 47 of the Charter'.[87] In contrast to that finding, the CJEU took issue with the ombudsperson's lack of independence from the executive,[88] and lack of power to adopt binding decisions on intelligence services.[89] The CJEU concluded that the Privacy Shield Decision was incompatible with Article 45(1) of the GDPR, read in light of Articles 7, 8 and 47 of the Charter and was accordingly invalid.[90]

Following the ruling, the DPC began an 'own volition' inquiry into the lawfulness of Facebook EU–US data transfers.[91] The DPC commenced the inquiry by issuing a 'Preliminary Draft Decision' (PDD) to Facebook. The PDD expressed the 'preliminary view' that Facebook EU–US data transfers failed to guarantee an 'essentially equivalent' level of data protection and that the DPC would consider proposing that the transfers be suspended.[92] In response, Facebook filed for judicial review arguing that the PDD violated fair procedures. The request for judicial review was rejected in May 2021.[93] Accordingly, the investigations into Facebook EU–US data transfers now continue apace with a decision by the DPC expected in the coming months. While the Facebook process may be ongoing, it is clear that the ruling in *Schrems II* has pressing implications for many more than the

[82] ibid para 180. The surveillance laws considered by the CJEU were the Foreign Intelligence and Surveillance Act Section 702 and Executive Order 12333 as limited by the Presidential Policy Directive 28.
[83] ibid.
[84] GDPR (n 4) art 45(2)(a).
[85] ibid rec 104; Case C-311/18 (n 13) para 188.
[86] See letter from US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, Decision 2016/1250 (n 50) Annex III.
[87] ibid recs 115 and 116.
[88] The Ombudsperson is appointed by and reports directly to the Secretary of State.
[89] Case C-311/18 (n 13) paras 195–7.
[90] ibid paras 198–201.
[91] Pursuant to Article 60 GDPR and Section 110 of the Data Protection Act 2018.
[92] *Facebook Ireland Limited v Data Protection Commission* [2021] IEHC 336 (14 May 2021).
[93] ibid.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

parties to the case and that all EU–US data exporters have complex matters to consider.

III. THE IMPLICATIONS OF *SCHREMS II*

In addition to the invalidation of the Privacy Shield, and the questions raised about the workability of SCC, it is clear that the reasoning of the CJEU in *Schrems II* also creates challenges for EU–US data transfers made in reliance on other mechanisms, including BCR. The position of the CJEU as regards the US surveillance programmes creates a potentially insurmountable obstacle to EU–US data transfer in the form it has existed in up until this point. The economic importance of transatlantic data flow has led to some calls for a third attempt to develop a new mechanism specifically for EU–US data transfers.[94] The US Department of Commerce and the European Commission recently released a statement committing to intensifying negotiations on an enhanced EU–US Privacy Shield framework to comply with the *Schrems II* ruling.[95]

In light of the robust stand taken by the CJEU in its case law, it is questionable whether this will be a fruitful path. One argument in favour of returning to the negotiation table is that the CJEU judgment in *Schrems II* appears to leave scope for the formulation of a data transfer agreement that could withstand CJEU scrutiny. As opposed to *Schrems I*—which includes harsh criticism of generalised surveillance measures as compromising 'the essence' of Article 7 CFR—the CJEU in *Schrems II* focuses on the absence of adequate safeguards.[96] While one could argue that generalised surveillance inherently lacks proportionality and sufficient safeguards, an agreement based on enhanced safeguards and remedies is imminently more reachable than an agreement on those things *in addition* to the total cessation of generalised surveillance of data originating from the EU. Such a reading would still require a significant shift in the CJEU position on generalised surveillance and in the US approach to enforcement and remedies for EU data subjects, however.

[94] J Meltzer, 'The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security' (*Brookings*, 5 August 2020) <https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/>; American Chamber of Commerce to the European Union *et al.*, 'Joint Industry Letter on Schrems II Case Ruling to European Commissioner Reynders, Secretary Ross, and European Data Protection Board Chairwoman Dr Jelinek' (30 July 2020) <https://www.itic.org/policy/JointIndustryLetterSchremsII-30July.pdf>.

[95] 'Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Gina Raimondo' (*European Commission*, 25 March 2021) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443>.

[96] T Christakis, 'After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe' (*European Law Blog*, 21 July 2020) <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/>.

https://doi.org/10.1017/S0020589321000348 Published online by Cambridge University Press

The emphasis on government surveillance in both *Schrems* cases has attracted criticism from US commentators in light of the significant commonalities between the US and many EU Member States on this point.[97] While this does not affect the fact that the EU legal order requires the fundamental rights of EU data subjects to be respected regardless of where their data travels, it could be seen as providing some common ground from which a mutually satisfactory agreement could be reached. In line with this, Cole and Fabbrini make the case for a comprehensive transatlantic privacy compact that would provide reciprocal protection of the data privacy rights of data subjects in both jurisdictions.[98] While a comprehensive privacy agreement would resolve some of the challenges posed by the 'un-territoriality of data', striking such a complex agreement between the US and the EU would be a remarkable achievement. It should also be noted that any agreement would have to respect the constitutional principles of the EU as set out in its foundational treaties.[99] Taking a broader view, Brown *et al.* have made the point that a multilateral treaty could resolve these issues and address the 'lacuna in human rights protection caused by foreign intelligence gathering and exchange', but such an agreement is even less likely than a bilateral compact.[100]

Even if a new agreement of any sort, including an updated Privacy Shield, is possible, the complexity of the task means its negotiation will take time. Moreover, while a grace period was granted to data exporters by the EDPB following the ruling in *Schrems I*; the CJEU has cast doubt on such a possibility this time, suggesting that the existence of derogations under Article 49 GDPR prevents the creation of a legal vacuum.[101] The need for short-term solutions calls for consideration of the viability of SCC post-*Schrems II* and what can be done to remedy gaps in protection for personal data when transferring to third countries.[102] Acknowledging that SCC cannot

[97] 'US Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows' (*U.S. Mission to the European Union*, 16 July 2020) <https://useu.usmission.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/>; P Swire, '"Schrems II" Backs the European Legal Regime into a Corner — How Can it Get Out?' (*IAPP*, 16 July 2020) <https://iapp.org/news/a/schrems-ii-backs-the-european-legal-regime-into-a-corner-how-can-it-get-out/>; S Baker, 'How Can the U.S. Respond to Schrems II?' (*Lawfare*, 21 July 2020) <https://www.lawfareblog.com/how-can-us-respond-schrems-ii>.

[98] D Cole and F Fabbrini, 'Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders' (2016) 14 ICON 220, 235.

[99] Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission* EU:C:2008:461.

[100] I Brown *et al.*, 'Toward Multilateral Standards for Foreign Surveillance Reform' in R Miller (ed), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017) 461–91.

[101] Case C-311/18 (n 13) para 202. The EDPB has advised caution regarding the use of Article 49 GDPR derogations, asserting that derogations: 'need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test'.

[102] Case C-311/18 (n 13) paras 132–7, referencing GDPR (n 4) rec 109.

bind the public authorities of third countries, the CJEU asserts that supplementary measures can be used to bring the level of protection up to the level required through the provision of additional safeguards where necessary.[103]

The ruling in *Schrems II* does not set out what the additional safeguards should be and it is clear that such measures will have to be identified on a case-by-case basis with due regard to all the circumstances of the transfer and the law of the third country. Supplementary measures may be contractual, technical, or organisational in nature. The European Data Protection Board (EDPB) highlights the limitations of contractual and organisational measures in its Recommendations on this issue and notes that such measures will, in general, not be sufficient to remedy challenges created by third country law but that they may complement technical measures.[104] Supplementary technical measures that could potentially prevent US agencies from accessing EU data include: end-to-end encrypting data and ensuring that the decryption key is only held by the EU-based data exporter; anonymising data (which would render the data outside the scope of EU data protection law); and pseudonymising data where only the data exporter has the capability to re-identify the data. It should be remembered, however, that the usability of encrypted data is very limited and thus the purpose of transferring the data may be thwarted as a result.[105] Moreover, the effectiveness of encryption as a safeguard relies on the belief that US intelligence agencies will not be able to penetrate the encryption.

Another solution touted to address the challenges identified in *Schrems II* has been data localisation. For example, the Berlin Supervisory Authority advises that until US law is reformed, EU personal data should not be transferred to the US.[106] While there is some political support for data localisation as a solution to international data transfer challenges,[107] simply storing data in Europe will likely not be sufficient due to the potential for extraterritorial access by US

[103] ibid paras 132–7.

[104] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (Adopted on 10 November 2020) 15–16 <https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf>.

[105] M Veale, R Binns and J Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 IDPL 105.

[106] Berliner Beauftragten für Datenschutz und Informationsfreiheit, 'Nach Schrems II: Europa Braucht Digitale Eigenständigkeit' (17 July 2020) <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf>; V Bensinger *et al.*, 'The End of Privacy Shield: European Data Protection Authorities React' (*National Law Review*, 21 July 2020) <https://www.natlawreview.com/article/end-privacy-shield-european-data-protection-authorities-react>.

[107] See, for example, A Kayali and F Eder, 'Thierry Breton "Understands" Trump on TikTok, wants Data Stored in Europe' (*Politico*, 1 September 2020) <https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/Breton>.

authorities.[108] Following the Snowden revelations, some went so far as to advocate for a separate communication network inside Europe to offer security for EU users.[109] Even if this is technically feasible, it is unclear whether it would be sufficient to prevent NSA access and the economic costs would be immense.[110]

Microsoft previously attempted to have data stored by a German company in order to keep European data in Europe and beyond the reach of US law enforcement.[111] The service was stopped, however, on the grounds that it was 'over-priced, under-performing and unpopular with customers'.[112] Since *Schrems II*, Microsoft have renewed focus on data localisation[113] and the French government have proposed a licencing system to provide for the continued use of cloud services (such as those provided by Microsoft) where the servers are located domestically and the data is stored and processed by European licensees.[114] With the outcome in *Schrems II*, the compliance benefits for large US technology companies might now outweigh the issues that lead to Microsoft's previous abandonment of the licensing model. It is notable that in a recently adopted Resolution, the European Parliament deems it necessary to support investment in European data storage tools to reduce the dependence on companies operating in jurisdictions, such as the US, with 'marked gaps' in data protection.[115]

IV. CONCLUSION

Even though there is strong political desire for a generally applicable agreement for EU–US data transfers, it seems that—absent a radical reform of US law—

[108] J Poortvliet, 'European Datacenter is No Solution, Recent Developments Show' (*Next Cloud*, 17 August 2017) <https://nextcloud.com/blog/european-datacenter-is-no-solution/https://nextcloud.com/blog/european-datacenter-is-no-solution/>; 'Next Steps for EU Companies & FAQs' (*noyb*, 20 July 2020) <https://noyb.eu/en/next-steps-eu-companies-faqs>.

[109] 'Merkel, Hollande to Discuss European Communication Network Avoiding US' (*Reuters*, 15 February 2014) <https://www.reuters.com/article/us-germany-france/merkel-hollande-to-discuss-european-communication-network-avoiding-u-s-idUSBREA1E0IG20140215>.

[110] Cole and Fabbrini (n 98) 235–6.

[111] J Poortvliet, 'Microsoft and Telekom No Longer Offer Cloud Storage Under German Jurisdiction' (*Next Cloud*, 4 September 2018) <https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction/>.

[112] C Kermann, 'Microsoft and Deutsche Telekom's "German Cloud" Wafts Away' (*Handelsblatt*, 13 March 2018) <https://www.handelsblatt.com/english/companies/remote-access-microsoft-and-deutsche-telekoms-german-cloud-wafts-away/23581454.html?ticket=ST-1495989-vsYxGyRenhSfQvKqgNqq-ap6>.

[113] B Smith, 'Answering Europe's Call: Storing and Processing EU Data in the EU' (*Microsoft EU Policy Blog*, 6 May 2021) <https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>.

[114] M Rosemain, 'France Embraces Google, Microsoft in Quest to Safeguard Sensitive Data' (*Reuters*, 17 May 2021) <https://www.reuters.com/technology/france-embraces-google-microsoft-quest-safeguard-sensitive-data-2021-05-17>.

[115] European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)) para 26 <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf>.

transfers to the US will have to be assessed on a case-by-case basis. Some industries will be affected more than others—electronic communication providers in particular. Technological solutions like encryption will be useful in some contexts and not in others. Data localisation will address some concerns. As discussed, there is some potential for cloud service providers to put European data out of the reach of US agencies, but additional challenges exist for global social network services that rely on 'multiway' as opposed to 'person-to-person' communication.[116] Many proposed solutions are also likely to entail significant costs that threaten the feasibility for data exporters.[117] Accordingly, there is, at this point, no generalisable solution that will remedy the EU–US data transfer challenge. However, if a technical solution is found, or if data localisation is adopted on a mass scale, an interesting unintended side effect of the ruling in *Schrems II* could be a reduction in the regulatory influence of the EU worldwide. While such a solution is difficult to imagine at present, Kuner goes so far as to speculate whether:

> the judgment may cause some third countries to question whether it is worthwhile to strive to reach the EU's data protection standards and to engage in protracted negotiations only to have the agreement, or the adequacy decision based on it, invalidated later on.

The Commission has consistently placed significant value on the spread of European data protection ideas and ideals globally. This is evidenced from the value it places on 'the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region' when assessing with which countries a dialogue on adequacy should be pursued.[118] The decision of the CJEU in *Schrems II* (and *Schrems I* before it) reduces the certainty associated with adequacy determinations and this, in turn, detracts from the value of entering into lengthy adequacy negotiations with the EU Commission.

Despite key tension points remaining consistent between the US and the EU, there have also been notable shifts in perception. Consider the comments of the lead negotiator of the Safe Harbour Agreement, David Aaron, made in 1999:

> these safe harbor principles have been developed and are aimed at a specific situation - reassuring the Europeans that their privacy…will be protected… In no way does the US government intend for these safe harbor principles to be seen as precedents for any future changes in the US privacy regime.[119]

[116] I Brown, 'Schrems II (the Revenge of Snowden) and a Facebook Restructuring?' (*Ian Brown*, 19 July 2020) <https://www.ianbrown.tech/2020/07/19/59/>.

[117] ibid.

[118] 'Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers' (*European Commission*, 10 January 2017) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15>.

[119] D Aaron, 'Remarks Before the Information Technology Session of America' (Fourth Annual IT Policy Summit, 1999) 4–5; S Kobrin, 'Safe Harbours Are Hard to Find: The Trans-Atlantic Data

While there is still no federal comprehensive data privacy law in the US, attitudes on the desirability of such a regime have evolved. Indeed, much of the current momentum for a federal data privacy law is driven by the adoption of comprehensive data privacy laws by numerous state legislatures.[120] The current tensions centre more on having the EU interfere with US intelligence practices rather than a general antipathy to technologically neutral data privacy protections. This is the case to the extent that many of the most affected companies now endorse federal data privacy rules.

While interest in a federal EU-inspired data protection law continues, the issues raised by the CJEU in *Schrems II* will not be addressed by a federal data privacy law without other more politically contentious reforms. This article has shown how the *Schrems II* decision leaves the future direction of travel somewhat uncertain. Due to the emphasis of the judgment on the disproportionality of the US government surveillance regime and the absence of effective remedies for EU data subjects, it is clear that major reform of some highly sensitive areas of US legal practice will be required to facilitate a general agreement on EU–US data transfers. In the absence of such an agreement, tailored solutions and safeguards will be required to facilitate transfers on a more targeted basis. In some instances, transfers will simply not be possible in a manner that complies with EU law read in light of the Charter.

Privacy Dispute, Territorial Jurisdiction and Global Governance' (2004) 30 Review of International Studies 111.

[120] M Noordyke, 'US State Comprehensive Privacy Law Comparison' (*IAPP*, 28 July 2021) <https://iapp.org/resources/article/state-comparison-table/>.