INSIGHT

SCHREMS II: EVERYTHING IS ILLUMINATED?

RÓISÍN ÁINE COSTELLO*

ABSTRACT: The decision in *Schrems II* delivered by the Court of Justice in July 2020 (judgment of 16 July 2020, case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*) was, in many ways, foreseeable given the scheme and recent history of the Union's privacy and data protection jurisprudence. Despite this, the decision has significant and far-reaching implications both for the protective standards afforded to personal data which are the subject of international data transfers and the role and responsibilities of data controllers where such transfers take place. More fundamentally, the decision also raises a series of further questions about the scope and reach of European data protection standards, the interpretation of the general Data Protection Regulation (GDPR) and the prospects of the United Kingdom in seeking an adequacy decision as a third country following Brexit.

KEYWORDS: data protection – privacy shield – safe harbour – GDPR – rule of law – *Schrems*.

I. INTRODUCTION

The decision in *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (*Schrems II*)[1] delivered by the Court of Justice in July 2020 was, in some ways, foreseeable given the recent history of the Union's privacy and data protection jurisprudence. Yet, the decision nevertheless has significant and far-reaching implications.

In particular, while the case has clarified and developed some aspects of the interpretation of the General Data Protection Regulation (GDPR) (notably in the relationship between the Charter of Fundamental Rights of the European Union, hereinafter the Charter, and the Regulation as well as the interdependent reading of the provisions of Chapter V) it also obfuscates the circumstances in which Standard Contractual Clauses (SCCs) may be relied on, introducing the new concept of "supplementary measures" whose practical function and form are left to the reader's imagination. The apparent development of a parallel system of data controller led 'mini' adequacy decisions pre-

* Ph.D. Candidate, Assistant Professor of Law, Dublin City University, roisin.ainecostello@dcu.ie.

[1] Court of Justice, judgment of 16 July 2020, case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (*Schrems II*), para. 80.

ISSN 2499-8249
doi: 10.15166/2499-8249/396

sents similar problems – further muddying rather than clarifying the precise delineation of obligations under the scheme of the GDPR.

This, perhaps, can be understood as contributing to the divergent reception which the judgment received in European and US circles with officials in the latter jurisdiction viewing the decision as leaving significantly more scope to continue relying on existing transfer mechanisms than their European counterparts understood as permissible.

What is clear from the judgment, however, is the increasingly strident approach taken by the Union in exercising data sovereignty and the arguably unsustainable dictating to third countries on both substantive and procedural requirements. In this respect, the judgment also (unintentionally) draws attention, on a close reading, to the differences in attitude of the Union to the surveillance schemes of Union Member States and third countries.

II. *Schrems I* and the background to *Schrems II*

Schrems II is the most recent decision in a series of linked cases taken by Maximillian Schrems against the Irish Data Protection Commissioner and resulting from preliminary references from the Irish courts to the Court of Justice. These cases began in 2013 when Mr Schrems challenged the transfer by Facebook Ireland of his personal data to servers belonging to its parent company Facebook Inc., located in the United States. Mr. Schrems lodged a complaint concerning this transfer with the Irish Data Protection Commissioner (DPC) under the Data Protection Directive[2] seeking to prohibit the transfer of his personal data to the United States by Facebook. Mr. Schrems sought the order on the basis that the law of the United States did not offer sufficient protection to personal data in the context of various surveillance and monitoring practices undertaken as part of that jurisdiction's national security measures.[3]

The DPC rejected Mr. Schrems' complaint on the basis that subsequent to Decision 2000/520 (the Safe Harbour Decision),[4] the European Commission had found that the United States did ensure an adequate level of protection to personal data transferred to that jurisdiction. Mr. Schrems sought a judicial review of the DPC's rejection. During these proceedings the Irish High Court referred several questions to the Court of Justice in October 2015. In its ruling on those questions in *Schrems I*[5] the Court of Justice de-

[2] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

[3] Court of Justice, judgment of 6 October 2015, case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*).

[4] Commission Decision 2000/520 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.

[5] *Schrems I*, cit.

cleared that the Safe Harbour Decision was invalid on the basis that it failed to ensure the required degree of comparable and adequate protection of personal data transferred to the United States.[6]

The Privacy Shield Decision replaced the Safe Harbour Decision following this finding and sought to improve some of the former Decision's weaknesses – including through the introduction of an Ombudsman system to ensure independent oversight. Crucially, however, there was little if any change to the State surveillance operating in the background of either Decision. In addition to this development and subsequent to the decision in *Schrems I*,[7] the GDPR was introduced and provided that personal data could be transferred to a third country (i.e. out of the Union) only in certain circumstances as set out in Chapter V of that Regulation.

In accordance with the provisions of Chapter V a third country may benefit from an 'adequacy decision' per Art. 45 which provides that data can be transferred to that jurisdiction on the basis that the third country has been certified by the Commission as ensuring a roughly equivalent level of protection to that afforded by the GDPR.[8] In the absence of an adequacy decision, a transfer of data can take place only if the personal data exporter has provided and ensured the application of appropriate safeguards for the transferred data in accordance with Art. 46.[9] Such safeguards have generally taken the form of standard data protection clauses adopted by the Commission[10] and which are included in contractual agreements concluded between the transferor (the data controller) and transferee according to the Standard Contractual Clause (SCC) Decision.[11]

Following the decision in *Schrems I*, Facebook Ireland began to transfer data to the United States using the second of these options – relying on standard data protection clauses set out in the Annex to the Privacy Shield Decision. The Irish High Court annulled the DPC's previous decision rejecting Schrems' complaint and referred the case back to the DPC for consideration in the context of the new legal landscape.

The DPC asked Mr. Schrems to reformulate his complaint given the invalidity of Safe Harbour and the new legal landscape for the transfer of personal data. In his reformulation

[6] *Ibid*., para. 98.

[7] 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).

[8] *Ibid*., Art. 45.

[9] *Ibid.*, Art. 46, para. 1.

[10] *Ibid*., Art. 46, para. 2.

[11] Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (as later amended by Commission Decision 2016/2297). Crucially, the Privacy Shield Decision interacts somewhat unusually with the GDPR. The United States has not received an adequacy ruling from the European Union. In that context, Safe Harbour and then Privacy Shield operated to enable participating companies in the United States to satisfy the requirements established by Chapter V of the GDPR.

Mr. Schrems alleged that Facebook's use of SCCs as approved by the Commission's SCC Decision and the new Privacy Shield decision could not provide a valid legal basis for transfers to the United States. Mr Schrems based this allegation, in part, on the fact that US law continued to oblige Facebook to make the personal data it held available to government authorities in the context of State surveillance programs and continuing shortcomings in the protections afforded to personal data under the United States' surveillance regime.

The DPC found it could not make a decision on the allegations contained in this new complaint in the absence of a decision on the validity of the Privacy Shield and the SCC Decision on the basis of which Facebook was now transferring data to the US. The DPC thus brought proceedings before the Irish High Court which in turn referred eleven questions to the Court of Justice by way of preliminary reference. These eleven questions can be broadly grouped into five broader issues concerning,

- whether the GDPR applies to data transfers when the data are likely to be processed in a third country for security and law enforcement purposes;[12]

- what level of protection applies to data processed pursuant to SCCs under the GDPR and whether that level of protection is to be read in accordance with the Charter, ECHR or national law;[13]

- whether the SCCs are valid in light of Arts 7, 8, and 47 of the Charter;[14]

- whether national data protection authorities (DPAs) are required to suspend or prohibit data transfers under the SCCs if they conclude the clauses are not complied with or the level of protection cannot be ensured; and[15]

- whether the Privacy Shield ensures an adequate level of protection for transferred data.[16]

III. The judgment of the Court of Justice in *Schrems II*

In answering these questions, the Court of Justice in *Schrems II*[17] dealt concisely with the first question concerning the applicability of the GDPR. This question was premised on the argument that as national security lies beyond the scope of the GDPR, questions concerning the processing of data for the purpose of public security, defence, and State security should be similarly considered to be outside the scope of the Regulation and its requirements. [18] The Court held that the fact that Art. 4, para. 2, TEU placed national se-

[12] *Schrems II*, cit., para. 80.
[13] *Ibid*., para. 90.
[14] *Ibid*., para. 122.
[15] *Ibid*., para. 106.
[16] *Ibid*., para. 160.
[17] *Ibid*.
[18] *Ibid*., paras 82-85.

curity matters within the exclusive purview of the Member States did not affect the applicability of the GDPR.[19]

Having affirmed the applicability of the GDPR, the Court proceeded to consider the level of protection applicable to data processed under the SCCs. The Court confirmed that the requirement for 'essential equivalence' with EU law under Art. 45 GDPR applied equally to the SCCs under Art. 46.[20] In particular, the Court noted that the comparator within EU law to be used when assessing essential equivalence was the GDPR read in light of the Charter (and not Member State law – a possibility which had been raised by the Irish DPC).[21]

The Court specified that in assessing whether the level of protection afforded by SCCs satisfied the requirement for 'essential equivalence' parties should afford particular consideration to both the clauses themselves and the relevant aspects of the legal system of the third country to which data was being transferred, as well as those matters set out in the non-exhaustive list included in Art. 45, para. 2 GDPR.[22]

This leads naturally to the question of which actors are tasked with assessing the equivalence of the protections afforded in third countries and what actions DPAs are required to take where they become aware such protections are not operating. The judgment in *Schrems II* is particularly notable in this regard, augmenting (or perhaps amending) the obligations placed on both data controllers and national data protection authorities to prospectively monitor and enforce compliance with protections that purport to afford essentially equivalent protections and ensuring that such essentially equivalent protections are present.

In assessing these considerations the Court first noted that national DPAs are responsible for monitoring compliance with EU law and the requirements of the GDPR and enjoy significant investigative powers under Arts 51 to 57 GDPR.[23] In particular, the Court confirmed that under Art. 46 GDPR, DPAs are obliged to suspend or prohibit data transfers if the agreed SCCs cannot be complied with or if protection of the data at issue cannot be otherwise ensured.[24] The Court also noted that the Commission's competence to draft SCCs does not restrict the powers of national authorities to review compliance in this way.[25]

[19] *Ibid*., para. 81. The Court did not distinguish, as AG Øe had, between "processing consisting in the transfer itself" and subsequent processing by national security authorities of a third country (see para. 104 of the Opinion), instead finding that the possibility of such subsequent processing was not relevant in light of Art. 45 GDPR (see para. 87).

[20] *Schrems II*, cit., para. 96.

[21] *Ibid*., paras 99-100.

[22] *Ibid*., paras 105.

[23] *Ibid.*, paras 107 and 119.

[24] *Ibid*., para. 113.

[25] *Ibid*., para. 115. In this, the Court's approach is broadly similar to that of AG Øe. In circumstances where data is transferred on the basis of an adequacy decision rather than SCCs, the Court of Justice con-

In addition to more clearly defining the obligations of DPAs, in this respect, the Court also noted that an SCC Decision imposes an obligation on data exporters and recipients, prior to any transfer, to verify that the required level of protection would be respected in the third country in which the recipient is located.[26] Furthermore, the recipient of data must inform the data controller of any inability they encounter in complying with the SCCs. On being informed of such an inability, the data controller is then obliged to suspend transfers and/or terminate the contract which permits the transfer of the data to the third country.[27]

Turning to consider the validity of SCC Decision itself, the Court noted that the crucial feature of the SCCs for the purposes of Mr. Schrems' complaint was that, as contractual standards subject to the doctrine of privity, they could bind only the parties to the agreement.[28] In upholding the use of SCCs the Court relied on Recitals of the GDPR[29] which they found supported a reading which foresaw the use of additional clauses or safeguards where the SCCs alone could not ensure the protection of personal data.[30]

This, equally, is an element of the decision which raises significant issues – not least what the necessary form and content of such additional measures would be and whether they can cure the deficiencies of a legal landscape in which there is neither an adequacy decision under Art. 45 and where SCCs alone are insufficient.

Turning to the Privacy Shield Decision, AG Øe in his Opinion had proffered arguments on basis of which the Court could have avoided having to address the validity of the Privacy Shield altogether.[31] However, the Court of Justice, contrary to the AG, found it had no choice but to address the validity of the Decision.[32]

The Court imposed the same analytical framework in assessing Privacy Shield as it had in addressing the SCC Decision – emphasising that the GDPR should be understood and read in light of the Charter and the rights in Arts 7, 8, and 47.[33] In assessing the Privacy Shield Decision, the Court noted that it granted primacy to the requirements of US national security and law enforcement, which the Court of Justice interpreted as condoning interference with the fundamental rights of those persons whose data were transferred to the US.

While the Court noted that interferences with the rights protected in Arts 7 and 8 were not *prima facie* impermissible, it found that based on the evidence which had been

firmed that a valid adequacy decision remains binding until it is declared otherwise but noted that this does not stop individuals from being able to complain (see para. 121).

[26] *Ibid*., paras 128-130 and 134.

[27] *Ibid*., para. 135.

[28] *Ibid*., para. 126.

[29] Recital 108 and 114 GDPR. See *Schrems II*., cit., para. 131.

[30] *Schrems II*, cit., para. 132.

[31] *bid.*, paras 174-186.

[32] *Ibid*., para. 151.

[33] *Ibid*., para. 122 *et seq*.

furnished to the Court, access to, and use of, personal data by US authorities was not limited in a way which satisfied the requirement for essential equivalence. In particular, the interferences were not limited to what was strictly necessary to achieve the legitimate objective[34] bur were instead disproportionate.[35] They were not necessary to genuinely meet objectives of general interest recognised by the Union, namely to protect the rights and freedoms of others,[36] nor was the scope of the interference they permitted defined.[37] The result, in the Court's assessment, was that access to and use of data under the Privacy Shield Decision were not circumscribed in a way that satisfied the requirements for essential equivalence.[38]

In particular, the Court noted that the provisions of both section 702 FISA and Executive Order 12333 were disproportionate. The former provision, in the Court's assessment, permitted only a review of the objectives of acquiring foreign intelligence rather than an assessment of whether individuals were properly targeted as part of attaining such objectives and conferred no justiciable rights.[39] Similar issues were raised, in the Court's assessment by the Executive Order.[40]

As a result, the Court found that the requirements of Arts 45, para. 2, let. a), GDPR and 47[41] of the Charter were not satisfied.[42] Most significantly, the Court noted that the Ombudsperson mechanism, introduced by the Privacy Shield Decision as a means of redress for the shortcomings identified in the Safe Harbour Decision, was insufficient to constitute an effective safeguard for the purposes of Art. 47 which would necessarily

[34] *Ibid*., para. 167 referring to the findings of the Commission in the Privacy Shield Decision. This is in line with Court of Justice: judgment of 9 November 2010, joined cases C-92/09 and C-93/09, *Volker and Schecke*, para. 48; judgment of 17 October 2013, case C-291/12, *Schwartz*, para. 33; judgment of 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01, *Rundfunk and Others*, paras 74-75; judgment of 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paras 33 and 36; opinion 1/15 of 26 July 2017, paras 124 and 126.

[35] These security measures included the PRISM and UPSTREAM surveillance programs. In relation to the former, Internet service providers are required, in accordance with court rulings, under section 702 FISA to supply the NSA with all communications to and from a 'selector' some of which are then transferred on to the CIA and FBI (see *Schrems II*, cit., para. 61). In relation to UPSTREAM, the NSA is given access to both the metadata but also the content of communications in internet traffic flows, in particular, Executive Order 12333 permits the NSA to access data in transit to the United States by accessing the underwater cables through which internet communications reach that jurisdiction (see *Schrems II*, cit., paras 62-65 and para. 184.

[36] *Ibid*., paras 174 and 183.

[37] *Ibid*., paras 175 and 181.

[38] *Ibid*., para. 185.

[39] *Ibid*., para. 179.

[40] *Ibid*., para. 184.

[41] Art. 47 requires that those whose rights or freedoms are violated be able to avail of an effective remedy and a hearing before an independent and impartial tribunal.

[42] *Schrems II*, cit., para. 186.

require that data subjects had judicial recourse based on actionable rights – which the Ombudsperson mechanism did not and could not provide.[43]

In particular, the Court noted that the Ombudsperson was unable to issue binding decisions directed toward the intelligence services, rendering it ineffective as a safeguard of the rights protected by Arts 7 and 8.[44] Given these findings, the Court ultimately invalidated the Privacy Shield[45] on the basis that the primacy of US law enforcement requirements[46] resulted in an inevitable failure of the limitations and safeguards necessary to establish that interferences with the rights protected by Arts 7, 8 and 47 were justified and that there could not be an essentially equivalent standard of protection for data subjects as a result.[47]

IV. Clarity, compromise and coming challenges

In some respects, the decision of the Court of Justice in *Schrems II* is unsurprising, continuing the active, and arguably strident, approach to ensuring the protection of personal data which characterised the Court's previous decisions in *Digital Rights Ireland*, followed by *Schrems I*, and the EU-Canada PNR Opinion. However, while the judgment in *Schrems II* continues this trend, it does so in ways which generates as many ambiguities as the case resolves.

The Court's confirmation that the GDPR should be interpreted in light of the Charter, for example, while welcome as an explicit articulation of a presumed interpretative approach, is far from revelatory. Yet the answers given by the Court on the application of protective standards, and what institutional actors are responsible for overseeing such decisions, seem to have muddied rather than illuminated contested areas of responsibility and enforcement.

Among the most novel aspects of the judgment was the Court's finding, concurring with the Opinion of AG Øe, that evaluating the adequacy of the protections in third countries to which data are transferred under SCCs, is a responsibility which falls to individual data controllers who, according to the Court's decision, must verify the existence of an adequate level of protection for individual data in the third country. [48]

This is surprising in light of the text of Art. 45 GDPR which appeared to reserve this responsibility to the Commission. The result is that the Commission's role in adequacy

[43] *Ibid*., para. 191 *et seq*.
[44] *Ibid*., para. 196.
[45] *Ibid*., paras 201-202.
[46] *Ibid*., para. 164.
[47] *Ibid*., paras 168-185.
[48] *Ibid*., para. 134.

decisions endures, however, apparently alongside a parallel system of *ad hoc*, small scale adequacy decisions made by data controllers.[49]

Quite aside from the obvious institutional confusion caused by this duplication of responsibility for the assessment of adequacy, this development significantly increases the expertise required of data controllers who must now possess not inconsiderable knowledge of the laws and policies which impact personal data in third countries. The real question must now be not whether such controllers are responsible for such assessments but how they can be – what enforcement powers will now be necessary to ensure controllers make such assessments and have the appropriate information and expertise to do so effectively.

In addition to this increased role for data controllers and the obligation, noted in Section II, for DPAs to take an active approach to halting data flows, the most significant development in *Schrems II* was the Court's interpretation of the provisions of Chapter V to create a common threshold for determining the presence of adequate protections of personal data – despite the differences in wording between Arts 45 and 46 GDPR.

Art. 45[50] requires "an adequate level of protection" with Art. 45, para. 2 going on to list the elements to be considered in determining whether such a level is present, including respect for the rule of law and human rights as well as "relevant legislation, both general and sectoral, including concerning public security, defence, national security, and criminal law and the access of public authorities to personal data". It was Art. 45, para. 2 which the Court of Justice interpreted in *Schrems I* as requiring a level of protection 'essentially equivalent" to that provided by EU law.

Art. 46, para. 1[51] meanwhile requires "appropriate safeguards", "enforceable data subject rights, and effective legal remedies for the data subject". These standards are, evidently, different from those in Art. 45. Yet in *Schrems II* the Court read Arts 45 and 46 in a complementary manner. In doing so, it imported the essential equivalence test and the accompanying factors to be taken into account from Art. 45 to the analysis used in determining the sufficiency of protections under Art. 46.

The Court justified reading Art. 46 in light of Art. 45 by noting that Art. 46 itself does not specify the nature of the requirements which flowed from its language but that, as the article appeared in Chapter V it should be read in light of Art. 44 which explicitly requires the provisions of Chapter V be applied in a manner which ensures the GDPR is not undermined.[52]

On this basis the Court found that the guaranteed standard of protection must subsist regardless of whether the transfer was completed pursuant to the mechanisms

[49] *Ibid*., para. 130.

[50] Deals with adequacy decisions.

[51] Is relevant to the alternative mechanisms by which transfers may take place.

[52] *Schrems II*, cit., para. 92 a position echoed by the AG at para. 117 of his Opinion.

under Arts 45 or 46. Intuitively this makes sense. The GDPR, after all, operates to ensure a consistent level of protection for the personal data of individuals regardless of their location or the mechanisms by which their data is transferred. The canons of interpretation both in civil and common law traditions would also support reading these clauses as forming part of a unitary, legislative whole rather than divisible and siloed provisions.

The less convincing portion of the judgment is the Court's finding in relation to the validity of the use of SCCs. While the Court, as it were, 'saved' the SCC Decision it did so by reference to a hypothetical the basis of which appears, at best, overly optimistic. Ultimately the Court held that, although there are situations in which the law and practices in force in a third country will permit the recipient of data to guarantee the necessary protection on the basis of SCCs, in the case before the Court they could not do so.[53]

More particularly the Court noted that, as SCCs cannot bind State parties it may prove necessary to supplement the guarantees contained in standard clauses with additional measures to ensure compliance with the required level of protection.[54] Yet it is unclear what supplementary measures precisely could be sufficient to convert transfers to a jurisdiction without an adequacy ruling, and with insufficient SCC protection, into acceptable transfers under the GDPR.[55] Neither did the Court enumerate what form or content would be necessary for such hypothetical supplementary measures to be effective or satisfactory in practice.[56]

The SCCs operate in those cases where a jurisdiction has not been granted an adequacy decision under Art. 45. This would tend to indicate that either the legal landscape or the practical operation of the law in that jurisdiction is such that the protection of personal data transferred there cannot be assured absent a supplementary mechanism (the SCCs). The Court has now held that the SCCs are not sufficient in themselves either and require further supplementary measures to be effective.

If those measures do not have the force of law, the capacity of State actors to bypass them or simply to depart from agreements to afford or enforce such measures – whether publicly or behind closed doors – makes their operation a matter of theory than practice. Alternatively, if the envisaged supplementary measures are more substantive and robust such that they cannot be so easily bypassed or disregarded, then they would likely be required to have the force of law. In that case, the jurisdiction's failure to secure an adequacy ruling to begin with would tend to indicate such measures are (despite having the force of law) insufficient to guarantee the appropriate standard of protection of personal data.

[53] *Ibid*., para. 126.

[54] *Ibid.*, paras 132-133.

[55] The United States' third-party doctrine most recently affirmed by the Supreme Court (albeit in a tepid judgment which may signal the doctrine's restriction) in the 2018 decision of *Carpenter v. United States* 138 US 2206 is perhaps the most striking example of how State actors can simply bypass measures not put on a strong legal footing.

[56] *Schrems II*, cit., para. 133.

The result is a hypothetical existence of supplementary measures which lends little further clarity to the relationship between adequacy decisions, the use of SCCs and the requirements which must or should exist to enable the latter transfer mechanism to meet the required levels of protection as an alternative to an adequacy decision.

It is only this obfuscatory proposal of theoretical supplementary measures which permitted the SCCs to "survive". By finding that supplementary measures may be required to ensure an adequate level of protection, the Court could nevertheless find that the SCC Decision itself includes mechanisms sufficient to make compliance with EU standards both possible and effective.[57] The result is a mere postponement of a more serious scrutiny of the use of SCCs and their legitimacy.

Interestingly this point, and the demise of Privacy Shield more generally, while widely acknowledged in academic circles, appear to have been less readily accepted by the US administration. The US Secretary of Commerce characterised the ruling as one which "appear[ed]" to have invalidated the Privacy Shield Decision and announced US businesses would continue to follow its requirements, making no mention of the insufficiency of the SCCs identified by the Court.[58]

This view is in stark contrast to that of the European Data Protection Supervisor[59] and the European Data Protection Board (the latter of which had long voiced concerns over the sufficiency of the protections afforded by Privacy Shield)[60] which recognised the decision as clearly invalidating Privacy Shield and requiring SCCs to be considered valid only in light of their broader context.[61] It appears that even in the reception of the judgment in *Schrems II* its protagonists are at cross purposes as to its outcome and its implications for their respective jurisdictions. This has been clearly illustrated by a challenge launched in the Irish High Court in September 2020 by Facebook which alleges that the Irish Data Protection

[57] *Ibid.*, para. 137. This implicit necessity for additional measures to operate alongside the SCCs to secure essential equivalence was also alluded to by the Council of Europe's Data Protection Commissioner in a joint statement with the Chair of the Council's Committee of Convention 108, noting that the decision raises broader issues about the transfer of data internationally and illustrated the need for Convention 108 – a binding international agreement on the protection of privacy and personal data. See Joint Statement by A. PIERUCCI, J-P. WALTER, *Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services*, 7 September 2020, rm.coe.int.

[58] US Department of Commerce, *US Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-US Data Flows*, 16 July 2020, www.commerce.gov.

[59] European Data Protection Supervisor, EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), 17 July 2020, edps.europa.eu.

[60] See European Data Protection Board, *EU-U.S. Privacy Shield – Second Annual Joint Review report*, 22 January 2019, edpb.europa.eu and European Data Protection Board, *EU -U.S. Privacy Shield – Third Annual Joint Review report*, 12 November 2019, edpb.europa.eu.

[61] European Data Protection Board, *Statement on the Court of Justice of the European Union Judgment in Case C-311/18 – Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, 17 July 2020, edpb.europa.eu.

Commission has no power to order the company to suspend transfers of data to the United States. The Commission had sent a preliminary order to Facebook directing the company to cease transferring data to the United States following the ruling by the Court of Justice in *Schrems II* which meant the mechanism used for transfer "cannot in practice be used".[62] Facebook has initiated a judicial review of the preliminary order, and has stated that the SCCs remain a valid mechanism for transfer subsequent to *Schrems II.*[63]

Some analysis of the outcome from a US perspective dwelt (unhappily) on the decision's imposition of European standards on non-Member States.[64] Such criticisms are, objectively, fair. The European Union is now engaged in exporting a system of rights protections which requires not only compliance with a system of proportional interference but a layered system of inquiry by both data controllers and the Commission into the minutia and broader context of data transfers – judging the treatment of personal data far beyond the Union, by the standards set in EU law.

The result is that international data transfers from the EU to third countries in the coming years look set to continue the "Brussels Effect"[65] – the regulatory trend which has seen European standards become the effective global standards for data protection as a result of market mechanisms[66] and diffuse cultural processes.[67]

The impact of this pattern beyond the borders of the Union has led Jack Goldsmith and Tim Wu to posit that the EU has become an 'effective sovereign' of data protection and privacy.[68] The decision in *Schrems II* only reinforces this perception – most notably through the findings made in the ruling on the lack of judicial review or other oversight of the surveillance mechanisms operating in the United States and the absence of sufficient vindication of individual rights. Such features, the Court noted, were necessary to ensure compliance with EU law but – more fundamentally – were "inherent in the existence of the Rule of Law".[69]

[62] S. SCHECHNER, E. GLAZER, *Ireland to Order Facebook to Stop Sending User Data to US*, *The Wall Street Journal*, 9 September 2020, www.wsj.com.

[63] S. MCDERMOTT, *Facebook launches High Court challenge to DPC's order to suspect EU-US data transfers*, *The Journal*, 11 September 2020, www.thejournal.ie.

[64] See for example the analysis offered by the former general counsel of the National Security Agency and Assistant Secretary for Policy at the Department of Homeland Security S.A. BAKER, *How Can the US Respond to Schrems II?*, *Lawfare*, 21 July 2020, www.lawfareblog.com.

[65] See A. BRADFORD, *The Brussels Effect*, in *North-Western University Law Review*, 2012, p. 107 *et seq.* See generally, *Why the whole world feels the 'Brussels effect'*, in *The Financial Times*, 16 November 2017; D. MICHAELS, *Hot US Import: European Regulations*, in *The Wall Street Journal*, 7 May 2018; A. SANTARIANO, *GDPR A New Privacy Law Makes Europe World's Leading Tech Watchdog*, in *The New York Times*, 24 May 2018.

[66] A. BRADFORD, *The Brussels Effect and the International Order*, www.law.columbia.edu.

[67] P.M. SCHWARTZ, *Global Data Privacy: The EU Way*, in *New York University Law Review*, 2019, p. 771 *et seq.*

[68] T. WU, J. GOLDSMITH, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford: Oxford University Press, 2006, p. 176.

[69] *Schrems II*, cit., para. 187.

It thus appears that not only procedural rights but also systemic adherence to democratic principles as articulated by the European Union are now required for a third country to be considered to have afforded sufficient protection to the rights of data subjects. It also raises significant questions over the ability of controllers to transfer data to third countries whose governments do not display an allegiance to the Rule of Law and the transparent, predictable, and prospective application of the law it requires.

While adherence to the Rule of Law is of course desirable, the evolution of the Brussels Effect from a regulatory trend to a means of exporting a prescriptive formula for adherence to democratic features of government and the ordering and substantive content of another jurisdiction's legal regime is of questionable value in either asserting the legitimacy of the Union's own legal ordering or in fostering sustainable models for bilateral agreement and relationships in a digital context.

In Europe, the judgment may prove particularly problematic in the context of the United Kingdom's departure from the Union. The United Kingdom presently operates an extensive surveillance regime under the Investigatory Powers Act 2016 which has already been the subject of repeated references to the Court of Justice (as well as the ECtHR) and is characterised by a similarly broad surveillance approach to that criticised by the Court in *Schrems II*.[70]

Crucially, and unlike the regime in place in the United States, the UK does have some oversight of surveillance and data collection operations in the form of an independent tribunal.[71] Nonetheless, bulk collection of data is permissible under the 2016 Act and, crucially, is applied differently to UK and non-UK citizens,[72] meaning it is questionable whether the Court of Justice would accept the operation of the scheme as necessary or proportionate – not least given the repeatedly voiced intention to repeal the Human Rights Act[73] which would cast the UK's commitment to human rights (a factor considered in Art. 45, and now also 46) into doubt.

The United Kingdom's data-sharing agreements with the United States may also cause concern in securing an adequacy decision following Brexit.[74] Indeed, a letter from

[70] A.D. Murray, *Data Transfers between the EU and the UK post Brexit?*, in *International Data Privacy Law*, 2017, pp. 158-162; A. Diker Vanberg, M. Maunick, *Data protection in the UK post-Brexit: the only certainty is uncertainty*, in *International Review of Law, Computers, and Technology*, 2018, pp. 191-193.

[71] Investigatory Powers Act 2000, section 65. Crucially this section will likely enjoy the reduced capacity to review complaints if, as promised, the Human Rights Act is repealed following Brexit.

[72] For a discussion of this see A.D. Murray, *Data Transfers between the EU and the UK post Brexit?*, cit., p. 163.

[73] For an examination of the likelihood of such a withdrawal and the UK's commitment to human rights more generally in the context of Brexit, see L. Moxham, O. Garner, *Will the UK uphold its commitment to human rights*, in *London School of Economics Blog*, 30 June 2020, blogs.lse.ac.uk.

[74] See Letter of the EDPB, edpb.europa.eu. Indeed, the decision in *Elgizouli v. Secretary of State for the Home Department* [2020] UKSC 10 is illustrative of these concerns. In that case, the transfer of personal data from UK and US in accordance with mutual legal assistance treaty in the context of a criminal investigation

the European Data Protection Board in June 2020 to Members of the European Parliament offers an insight into the Union's attitude to an adequacy ruling for the UK given its agreement with the US – noting doubts as to whether the safeguards in such agreement would be sufficient.[75]

A failure by the UK to obtain an adequacy decision or to provide sufficient supplementary safeguards alongside the SCCs to allow the transfer of data to the UK would be generally undesirable but would cause significant challenges on the island of Ireland where commitments to continued peace-building which includes infrastructural integration and intelligence sharing between the Republic of Ireland and Northern Ireland would face disruption in the event of data being unable to be moved from one jurisdiction to another.[76]

Surprisingly, the decision in *Schrems II* does not allude to the Court of Justice's most relevant decisions for the UK in this respect – the joined judgment delivered in *Tele2 Sverige* and *Watson*[77] which found the general and indiscriminate collection of personal data as part of national crime prevention strategies was contrary to EU law, in particular Arts 7 and 8 of the Charter. The omission of *Tele2 and Watson* from the decision is notable. AG Øe in his opinion adopted a view of the decisions in *Tele2 and Watson*[78] which appears to have been implicitly rejected, with the Court noting that national security does not oust the authority of the GDPR and declining to engage with its previous judgment in that case.

Equally, the absence might be read as the Court attempting to differentiate between a stricter approach to national data retention regimes and a more lenient approach to cases of data protection in the context of commercial data transfers which are subsequently accessed for national security purposes. If this is the case it signals a creeping inclination (evident to some extent in the dissent of Judge Vehabović in the ECtHR case of *Benedik v Slovenia*[79]) towards an understanding of privacy and data protection as being subject to a standard not entirely dissimilar to the US third party doctrine, with those data relinquished in return for access to online services considered, to a

was found by the Supreme Court to be unlawful as the transfer had not complied with the UK Data Protection Act 2018 which gave force to the jurisdictions EU law obligations in respect of data protection.

[75] See European Data Protection Board, *Letter to the Members of the European Parliament*, 15 June 2020, edpb.europa.eu.

[76] See The Institute for Government, *Operation Yellowhammer?*, 18 February 2020, www.instituteforgovernment.org.uk; J. PICKARD, *Yellowhammer document sets out potential damage of no-deal Brexit*, in *Financial Times*, 11 September 2019, www.ft.com; L. O'CARROLL, *Brexit 'could impede coronavirus contact tracing on island of Ireland*, in *The Guardian*, 1 May 2020, www.theguardian.com.

[77] Court of Justice, judgment of 21 December 2016, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*.

[78] *Ibid*., paras 219-220.

[79] European Court of Human Rights, judgment of 24 July 2018, no. 62357/14, *Benedik v. Slovenia*.

greater or lesser extent, to have been implicitly surrendered and subject to a reduced privacy expectation.

Certainly, such a shift, while unwelcome from an individual rights perspective, would seem to sit more coherently with the reality of the national security and surveillance landscape within the Union's Member States, several of which possess surveillance structures similar to those employed by the United Kingdom – a double standard to which the negotiations as to the UK's adequacy under the GDPR following Brexit are likely to bring unwelcome attention.

V. Conclusion

The invalidation of the Privacy Shield by the Court of Justice in *Schrems II* raises uncomfortable questions about the policy analysis and negotiation process which generates adequacy decisions within the Union. Many of the features which lead to Privacy Shield's invalidation were merely echoes of the same criticisms which had doomed Safe Harbour[80] while the changes (notably the introduction of the Ombudsman) appear to have been mere fig leaves – permitting the endurance of the previous regime which remained, unchanged in all but name.

A third agreement between the EU and US in the same vein (making minor changes to the Privacy Shield) would be neither credible nor sustainable and would, more fundamentally, damage the credibility of the Commission's independence and integrity in protecting citizens' rights in international negotiations.

The decision in *Schrems II* also leaves open perhaps more questions than it resolves. The decision exposes the theoretical difficulties of the Union's extra-territorial reach and its imposition of not only procedural but substantive legal requirements on third countries. It also highlights the contradictions which will likely be unravelled during post-Brexit adequacy negotiations between attitudes to and treatments of the surveillance practices of Member States (perhaps best characterised as a wilful ignorance) and third countries (as the attitude to the US practices illustrates).

In addition to these more theoretical difficulties exposed by the judgment, there are more prosaic shortcomings in its findings. The interpretation of the provisions of Chapter V and the relationship of the Charter to the interpretation of the GDPR have certainly been clarified. However, the dubious basis on which the SCC Decision endures, and the duplication of responsibility for adequacy assessments (now apparently split between data controllers and the Commission) are likely to lead only to further litigation as Facebook's pending High Court challenge in Ireland illustrates.

[80] *Schrems I*, cit., para. 86.