Developments

Reality and Illusion in EU Data Transfer Regulation Post *Schrems*

*By Christopher Kuner**

Abstract

The judgment of the Court of Justice of the European Union in *Schrems v. Data Protection Commissioner*, in which the Court invalidated the EU-US Safe Harbour arrangement, is a landmark in EU data protection law. The judgment affirms the fundamental right to data protection in the context of international data transfers, defines an adequate level of data protection, and illustrates how data protection rights under EU law can apply to data processing in third countries. It also raises questions about the status of other legal bases for international data transfers under EU law, and shows that many legal disputes concerning data transfers are essentially political arguments in disguise. The *Schrems* judgment illustrates the tendency of EU data protection law to focus on legalistic mechanisms to protect data transfers rather than on protection in practice. The EU and the US have since agreed on a replacement for the Safe Harbour (the EU-US Privacy Shield), the validity of which will likely be tested in the Court of Justice. Regulation of data transfers needs to go beyond formalistic measures and legal fictions, in order to move from illusion to reality.

* Professor of Law and Co-Chair of the Brussels Privacy Hub, Vrije Universiteit Brussel (VUB), Brussels; Affiliated Lecturer, Faculty of Law, University of Cambridge; Visiting Professor, Department of Law, London School of Economics and Political Science; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels. I am grateful for the useful comments on a previous version of this article by a number of colleagues, including Hielke Hijmans; Ira Rubenstein; participants in a seminar at the Centre for Intellectual Property and Information Law of the University of Cambridge; and officials of various data protection authorities. I also thank Anna Ciesielska for her valuable research assistance. This article is current as of June 2017.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

"Dearer to us than a host of truths is an exalting illusion."[1]

A. Introduction

In a world that has been transformed by the Internet, the ability to transfer personal data across national borders, and to access information regardless of geography, has become crucial for social interaction, economic growth, and technological advancement. At the same time, there is increased concern about the impact that the processing of personal data can have on individual rights, particularly when data are transferred globally. The most influential body of regulation protecting international data transfers is that contained in the European Union (EU) Data Protection Directive 95/46[2] (the "Directive"), which will be replaced by the new EU General Data Protection Regulation (the "GDPR")[3] on May 25, 2018. Both instruments restrict the transfer of personal data outside the EU.

On October 6, 2015, the Court of Justice of the European Union (CJEU) issued its most significant judgment to date dealing with EU data transfer regulation. In *Maximilian Schrems v. Data Protection Commissioner*,[4] the CJEU invalidated the decision[5] of the European Commission finding that the EU-US Safe Harbour agreement provided "adequate protection" for data transfers under Article 25 of the Directive. The *Schrems* judgment and the opinion of the Advocate General[6] that preceded it provoked an intense public reaction, including front-page articles in major international newspapers;[7] a press conference by top

---

[1] Anton Chekhov, *Gooseberries*, *in* SELECTED STORIES OF ANTON CHEKOV 5793, 5793–94 (Richard Pevear & Larissa Volokhonsky trans., Kindle ed. 2009) (paraphrasing Alexander Pushkin).

[2] Directive 95/46, of the European Parliament and of the Council 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 O.J. (L 281) 31 (EC).

[3] Regulation 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 [hereinafter GDPR], 2016 O.J. (L 119) 1 (Chapter V of the GDPR deals with international data transfers) (EU).

[4] ECJ, Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:6506, Judgment of 6 October 2015.

[5] Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7. The European spelling "Safe Harbour" is used throughout because that is used by the Court; the American spelling "Safe Harbor" is used when it appears as such in original sources.

[6] Opinion of Advocate General Bot, Case 362/14, Schrems v. Data Prot. Comm'r (Sept. 23, 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=297564.

[7] *See*, *e.g.*, Duncan Robinson, Richard Waters & Murad Ahmed, *US Tech Companies Overhaul Operations After EU Data Ruling*, FIN. TIMES (Oct. 6, 2015), http://www.ft.com/intl/cms/s/0/5d75e65a-6bf8-11e5-aca9-d87542bf8673.html#axzz3vvmklE7x; Mark Scott, *Data Transfer Pact Between U.S. and Europe is Ruled Invalid*, N.Y.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

officials of the European Commission;[8] reactions from US government officials;[9] opinions of academic experts;[10] legal memoranda from business groups;[11] and a newspaper interview by the president of the CJEU.[12]

On February 2, 2016, the EU and the US agreed on the EU-US Privacy Shield as a replacement for the Safe Harbour, and on July 12, 2016, the European Commission published a formal decision finding that the Shield provides a level of data protection that is "essentially equivalent" to that of EU law.[13] The Privacy Shield came into effect on August 1, 2016, and numerous US-based companies have already joined it.[14] The legal framework for data transfers from the EU to the US has been buttressed further by an international agreement[15] and related Council Decision[16] concerning data exchanges between law enforcement

---

TIMES (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0>.

[8] *See* European Commission Press Release, First Vice-President Timmermans and Commissioner Jourová's Press Conference on Safe Harbour Following the Court Ruling in Case C-362/14 (Schrems), (Oct. 6, 2015), http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.

[9] *See* Julie Brill, Former Comm'r, US FTC, Keynote Address Before the Amsterdam Privacy Conference, Transatlantic Privacy After *Schrems*: Time for an Honest Conversation (Oct. 23, 2015), https://www.ftc.gov/system/files/documents/public_statements/836443/151023amsterdamprivacy1.pdf; United States Mission to the EU, Safe Harbor Protects Privacy and Provides Trust in Data Flows that Underpin Transatlantic Trade, (Sept. 28, 2015), http://useu.usmission.gov/st-09282015.html.

[10] *See*, *e.g.*, *Debate: The Schrems Case*, VERFASSUNGSBLOG, http://verfassungsblog.de/category/schwerpunkte/the-schrems-case/; Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013* (Dec. 18, 2015), http://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf.

[11] *See* SIDLEY AUSTIN LLP, ESSENTIALLY EQUIVALENT: A COMPARISON OF THE LEGAL ORDERS FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND UNITED STATES (2016), http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf.

[12] *See* Valentina Popp, *ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust*, WALL ST. J. BLOG, (Oct. 14, 2015, 4:05 AM), http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/tab/print/.

[13] *See* Commission Implementing Decision 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-U.S. Privacy Shield, 2016 O.J. (L 207) 1, para. 137 (EU). The Privacy Shield has also been published in the US Federal Register. *See* Privacy Shield Framework, 81 Fed. Reg. 51,042 (Aug. 2, 2016).

[14] The list of companies that have joined the Privacy Shield can be consulted at https://www.privacyshield.gov/list.

[15] *See* Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses, U.S.-EU, Feb 1, 2017 O.J. (L 336) 3. The Umbrella Agreement entered into force on February 1, 2017.

[16] Council Decision 2016/2220 of 2 December 2016 on the Conclusion, on Behalf of the European Union, of the Agreement Between the United States of America and the European Union on the Protection of Personal

authorities (the so-called "Umbrella Agreement"), and changes to US law that grant additional data privacy rights to EU individuals.[17] Further judgments of the CJEU dealing with international data transfers are also forthcoming.[18]

The *Schrems* judgment is a landmark case that strengthens the fundamental right to data protection in EU law. In *Schrems*, the CJEU affirmed data protection rights with regard to data transfers; supported the right of data protection authorities (DPAs) to investigate the adequacy of protection for data transferred to third countries; and clarified what constitutes an adequate level of data protection under EU law. It is the first time the CJEU analyzed regulation of international data transfers in light of key provisions of EU treaty law such as the Treaty on the Functioning of the EU (the TFEU)[19] and the EU Charter of Fundamental Rights (the Charter).[20]

Further legal challenges to EU-US data transfer arrangements are ongoing. Thus, on May 24, 2016, the Irish Data Protection Commissioner referred questions to the Irish Commercial Court, a division of the Irish High Court, concerning the validity of the EU-approved standard contractual clauses for data transfers, which will likely result in a referral to the CJEU.[21] Challenges to the Privacy Shield have also been brought before the CJEU.[22]

There have been so many legal developments, political statements, and polemic arguments dealing with data transfers between the EU and the US, that it is easy to lose track of the larger issues at stake. Viewed from a high-level perspective—which I will refer to as the "meta level"—the *Schrems* judgment shows how the regulation of international data transfers in EU law is caught between reality and illusion. The main strand of the Chekhov story quoted at the beginning of this article involves a character who lives in the illusion that the fruits produced by his gooseberry bushes are sweet, while in fact they are unripe and sour. EU data protection law similarly maintains the illusion that it can provide seamless, effective protection of EU personal data transferred around the world, a view that the

---

Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2016 O.J. (L 336) 1 (EU).

[17] *See* Judicial Redress Act of 2015, H.R. 1428, 114th Cong. (2016).

[18] *See* Opinion of Advocate General Mengozzi, *Opinion 1/15*, (Sept. 8, 2016), ECLI:EU:C:2016:656, http://curia.europa.eu/juris/document/document.jsf?docid=183140&doclang=EN&mode=req&occ=first. The judgment in the case had not yet been issued when this article was published.

[19] Treaty on the Functioning of the European Union art. 15, Oct. 12, 2012, 2012 O.J. (C 326) 47.

[20] Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C 364/1) 389.

[21] *See* Data Prot. Comm'r v. Facebook Ir. Ltd. & Anor 2016/4809 P [hereinafter "Schrems II"].

[22] *See* Case T-670/16, Dig. Rights Ir. v. Comm'n, Sept. 16, 2016, O.J. (C 410) 26; Case T-738/16, La Quadrature du Net v. Comm'n, Oct. 25, 2016, O.J. (C 6) 39.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

Schrems judgment affirms. This is a beautiful illusion, at least to European eyes, because it envisions a world where the reach of EU data protection law extends globally; where attempts by foreign intelligence agencies to access the data of Europeans are repelled through the use of procedural mechanisms; and where DPAs police the Internet and quash attempts to misuse European data.

Yet it remains an illusion, as can be seen by the consequences of the *Schrems* judgment. Procedural mechanisms may satisfy formal requirements of data protection law, but they cannot provide protection against the intelligence surveillance that the *Schrems* case involved. Data localization attempts to minimize or avoid the transfer of personal data to third countries, but cannot protect data transfers on a broad scale. DPAs have a crucial role to play in the protection of personal data, but have a limited ability and willingness to enforce the law across borders, as shown by the fact that there has been very little enforcement related to the *Schrems* judgment.

In exploring the reality and illusion of protection for international data transfers, I will first summarize the CJEU's judgment in *Schrems*, before going on to examine its main holdings. In particular, I will analyze the CJEU's affirmation of the fundamental right to data protection and extension of its scope to third countries, its strengthening of the role of the DPAs, and its definition of an adequate level of data protection for data transfers. I will explain why the correct legal measure of adequate protection for international data transfers under EU law is the EU Charter of Fundamental Rights. I will also examine the concept of "essential equivalence" that the CJEU articulated, which both requires a high level of protection under the Charter, and raises questions as to how the DPAs and the courts will be able to cope with the burden that the CJEU has placed upon them.

I will then move to the meta level and discuss the implications of the *Schrems* judgment for the other data transfer mechanisms in the Directive and the GDPR, including the new Privacy Shield. I will show how legal issues of data transfer regulation are intertwined with the underlying political positions of the parties, and that the law cannot by itself provide a resolution of the disagreements between them unless they are willing to go beyond their preconceptions and consider the larger issues at stake. Finally, I will provide some suggestions on how to move the regulation of international data transfers from illusion to reality.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

B. The *Schrems* Judgment

I. Background and Facts

The facts of the *Schrems* judgment will be briefly summarized here. Further information about the background of the case and Schrems' allegations is provided on the plaintiff's web site,[23] and in the judgment of the Irish High Court that resulted in the reference for a preliminary ruling to the CJEU.[24]

Maximilian Schrems brought several complaints against Facebook before the Irish Data Protection Commissioner (DPC), based on, among other things, Facebook's membership in the Safe Harbour. Safe Harbour was a self-regulatory mechanism that US-based companies could join to provide protection for personal data transferred from the EU to the US. It was comprised of a set of principles based on EU data protection law with which Safe Harbour member companies had to comply, and was overseen by the US Federal Trade Commission (FTC) and US Department of Transportation (DOT). In 2000, the European Commission issued a formal decision under Article 25 of the Directive finding that transfers of personal data under the Safe Harbour provide adequate protection under EU data protection law.[25]

Following the Snowden revelations of 2013, which contained allegations of widespread surveillance of Internet data by US intelligence agencies, Schrems filed further complaints with the DPC, alleging that there was no meaningful protection in US privacy law and practice with regard to intelligence surveillance. The DPC took the position that under Article 25(6) of the Directive, it could not question the European Commission's determination of the Safe Harbour as providing adequate protection.[26] Schrems argued that the DPC should use its statutory powers to find that no adequate protection existed under the Safe Harbour,

---

[23] *See* Maximilian Schrems, EUROPE VERSUS FACEBOOK, "Legal Procedure against 'Facebook Ireland Limited'", http://europe-v-facebook.org/EN/Complaints/complaints.html, containing copies of the complaints against Facebook and other relevant documents in the case.

[24] *See* Schrems v. Data Prot. Comm'r [2014] 2 ILRM 441 (H. Ct.) (Ir.), [2014] I.E.H.C. 310; Schrems v Data Prot. Comm'r II [2014] 2 ILRM 506; [2014] I.E.H.C. 351.

[25] Commission Decision 2000/520, *supra* note 5.

[26] Article 25(6) of the Directive, *supra* note 2, provides as follows:

> The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

and that it should order Facebook to cease its data transfers to the US. In 2013, he sought judicial review in the Irish High Court against the DPC's decision not to proceed against Facebook. In his judgment of June 18, 2014, Mr. Justice Hogan of the High Court referred the following two questions to the CJEU:

> (1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding? (2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?[27]

On September 23, 2015, Advocate General Yves Bot delivered his opinion. The Advocate General found that:

> [T]he existence of a decision adopted by the European Commission on the basis of Article 25(6) of Directive 95/46 does not have the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred and, where appropriate, from suspending the transfer of that data.

Furthermore, the Advocate General held that the Safe Harbour decision of the European Commission should be held invalid.[28]

---

[27] Reference for a Preliminary Ruling from High Court of Ireland (Ireland), Case C-362/14, Schrems v. Data Prot. Comm'r (July 25, 2014), http://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=EN.

[28] Opinion of Advocate General Bot, *supra* note 6, at para. 237.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

II. Main Holdings

On October 6, 2015, the Grand Chamber of the CJEU issued its judgment. The CJEU broadly agreed with the conclusions of the Advocate General concerning the two questions put to it, finding that the DPAs were not prevented by Article 25(6) from examining claims related to the adequacy of protection under a European Commission decision, and that the decision underlying the Safe Harbour was invalid. The following were the main points that the CJEU made. In this section references in parentheses will be made to the relevant paragraphs of the judgment.

The CJEU first considered the powers of the national DPAs when the European Commission has issued an adequacy decision under Article 25(6) of the Directive. It found that all provisions of the Directive must be interpreted in light of a high level of fundamental rights protection under the Charter and the CJEU's case law interpreting the Charter (paragraphs 38–39). In considering the powers of the DPAs, the CJEU stressed the importance of their independence (paragraphs 40–43), and mentioned that their powers do not extend to data processing carried out in a third country (paragraph 44). It further held that the transfer of personal data to a third country is itself an act of data processing, and thus falls within Member State law (paragraph 45) and the supervisory powers of the DPAs (paragraph 47). Because a European Commission decision concerning adequacy under Article 25(6) of the Directive is binding on the Member States and must be given full effect by them, the DPAs cannot take measures contrary to such a decision (paragraph 52).

A European Commission decision cannot preclude an individual from filing a claim with a DPA concerning the adequacy of protection, nor can such a decision eliminate or reduce their powers (paragraphs 53–58). Such a claim is to be understood as essentially concerning "whether that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals" (paragraph 59). Only the CJEU has the power to declare an act by the EU invalid, including a European Commission adequacy decision (paragraph 61), and while national courts and the DPAs may consider the validity of an act by the EU, they may not themselves declare it invalid (paragraph 62).

Thus, when an individual makes a claim to a DPA contesting the compatibility of a data transfer based on an adequacy decision with the protection of privacy and fundamental rights, the DPA must examine the claim "with all due diligence" (paragraph 63). When the DPA rejects such a claim as unfounded, the individual must have access to judicial remedies allowing him to contest this decision before national courts, and such courts "must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded" (paragraph 64). Conversely, when the DPA finds such claim to be well-founded, it must "be able to engage in legal proceedings" (paragraph 65). As the Court stated in that paragraph, the national legislature must:

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

> Provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

The CJEU then considered the validity of the Safe Harbour itself, agreeing with Mr. Justice Hogan that it was necessary to consider this question in order to give a full answer to the questions referred (paragraph 67). The CJEU went on in paragraph 73 to find that, based on the EU Charter of Fundamental Rights, the term "an adequate level of protection" as used in the Directive must be understood as:

> Requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.

This definition does not require that the level be identical to that under EU law (paragraph 73). Without this requirement, "the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries" (paragraph 73). While the means to which a third country has recourse for ensuring a high level of protection may differ from those employed within the EU, they must prove to be effective in practice (paragraph 74).

Assessing the level of protection in a third country requires the European Commission to "take account of all the circumstances surrounding a transfer of personal data to a third country" (paragraph 75), to check periodically whether the adequacy assessment is still justified (paragraph 76), and to take account of circumstances that have arisen after adoption of the decision (paragraph 77). All this means that "the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict" (paragraph 78).

The CJEU then dealt with the validity of the Safe Harbour adequacy decision. While it found that "a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or . . . international commitments,'" the

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

reliability of such a system is based on "the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice" (paragraph 81). It noted that public authorities in the US are not required to comply with the Safe Harbour principles (paragraph 82), and that the Safe Harbour decision of the European Commission does not contain sufficient findings explaining how the US ensures an adequate level of protection (paragraph 83).

The CJEU stated that application of the Safe Harbour principles may be limited to meet, for example, national security, public interest, or law enforcement requirements (paragraph 84), and the decision states that "[c]learly, where US law imposes a conflicting obligation, US organisations whether in the Safe Harbour or not must comply with the law" (paragraph 85). It found that these provisions in effect give US law primacy over EU fundamental rights in situations where they conflict (paragraphs 86–87), and that to establish an interference with fundamental rights, "it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference" (paragraph 87). Moreover, the Safe Harbour decision does not contain any finding concerning limitations on the powers of public authorities (such as law enforcement authorities) in the US to interfere with fundamental rights (paragraph 88).

The CJEU then referred to previous statements by the European Commission that the US authorities were able to access data transferred to the US and process it in a way that is incompatible with the purposes of transfer and with the principles of necessity and proportionality (paragraph 90). It mentioned the need under EU law for there to be clear and precise rules regarding the scope of application of a measure and for effective protection against the risk of abuse of data (paragraph 91), and that derogations and limitations in relation to data protection should apply only when strictly necessary (paragraph 92). The CJEU did not explicitly state whether US law meets EU standards,[29] but there is no doubt that the judgment is based on a condemnation of US intelligence gathering practices and their effect on fundamental rights under EU data protection law,[30] as can be seen, for example, in the CJEU's mention of studies by the European Commission finding

[29] See Popp, *supra* note 12, for a statement of CJEU President, Koen Lenaerts, noting that "[w]e are not judging the U.S. system here, we are judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they be."

[30] *See, e.g.*, *Schrems*, *supra* note 4, at para. 93 (implying that data transferred to the US are subject to undifferentiated storage, access, and use, such as it criticized in ECJ, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland & Seitlinger, ECLI:EU:C:2014:238, Judgment of 8 April 2014) and para. 96–97 (finding that the Commission had not stated that the US law ensures an adequate level of data protection).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

that US authorities were able to access data in ways that did not meet EU legal standards in areas such as purpose limitation, necessity, and proportionality.[31]

The CJEU stated in paragraph 93 that:

> Legislation is not limited to what is strictly necessary where it authorizes, on a generalized basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.

It found that "legislation permitting the public authorities to have access on a generalized 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" (paragraph 94), and went on to state in paragraph 95 that:

> Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.

The CJEU went on to note that the European Commission did not state in its Safe Harbour decision that the US ensures an adequate level of protection (paragraph 97), and that the decision was accordingly invalid, without there being any need for it to examine the substance of the Safe Harbour principles (paragraph 98). Throughout this section of the judgment, the CJEU makes extensive reference to its earlier ruling in *Digital Rights Ireland*,[32] in which the CJEU strongly affirmed data protection rights in the digital context. The CJEU also found that Article 3 of the Safe Harbour decision contained impermissible limitations on the powers of the data protection authorities (paragraphs 99–104).

---

[31] *See id.* at para. 90.

[32] *See* Digital Rights Ireland & Seitlinger, *supra* note 30.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

C. Main Themes of the Judgment

The importance of the judgment rests in four main themes that the CJEU focused on and that will be discussed in turn.

I. Affirming the Right to Data Protection

The judgment strongly affirms data protection as a fundamental right under EU law. The CJEU makes repeated reference to fundamental rights under the Charter, and to previous data protection judgments such as *Digital Rights Ireland* and *Google Spain*.[33] This emphasis on fundamental rights is further demonstrated by the statement in paragraph 78 that the European Commission's discretion in judging the adequacy of protection in third countries should be "strict." The importance of the *Schrems* judgment for the protection of fundamental rights in the international context can also been seen in the frequent citations to it in the opinion of Advocate General Mengozzi of September 8, 2016, in a case concerning the validity of the draft agreement between Canada and the EU on the transfer and processing of airline passenger name record data.[34]

The CJEU found that generalized access to data by public authorities—for example, law enforcement authorities—compromises the essence of the right to private life under Article 7 of the Charter, but did not mention whether such access also violates the essence of the right to data protection under Article 8 of the Charter. The rights to data protection and privacy are closely linked, and surveillance by intelligence services self-evidently involves the processing of personal data. The CJEU's failure to mention the essence of the right to data protection may thus reflect its longstanding confusion about the distinction between the right to data protection and privacy.[35]

II. Application of Data Protection Rights to Third Countries

The CJEU indicated that while it was not directly applying EU law to third countries (paragraph 44), EU law did apply to data transfers under the Safe Harbour because "the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46."[36] In the end, the distinction between the direct application of EU law in

[33] ECJ, Case C-131/12, Google Spain v. AEPD and Mario Costeja Gonzalez, ECLI:EU:C:2014:317, Judgment of 13 May 2014.

[34] Opinion of Advocate General Mengozzi, *Opinion 1/15*, *supra* note 18.

[35] *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 270–272 (2015); Christopher Docksey, *Four Fundamental Rights: Finding the Balance*, 6 INT'L DATA PRIVACY L. 195, 198 (2016).

[36] *See Schrems*, *supra* note4, at para. 45.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

a third country and the transfer of EU-based data to such a country does not matter because in most cases transfers are only possible when the third country provides protections based on EU data protection standards. EU law thus applies indirectly to data processing in third countries via the mechanism of data transfer regulation.[37]

The Court's only previous case dealing specifically with regulation of international data transfers was its *Lindqvist* judgment of 2003,[38] in which it found that there is no data transfer to a third country within the meaning of Article 25 of the Directive when an individual in a Member State loads personal data onto an Internet page stored on a site hosted within the EU. The judgment in *Schrems* goes beyond *Lindqvist* by relating the requirement of an adequate level of data protection under the Directive to the level of data protection required by the Charter.[39] The CJEU thus requires a high level of data protection for data transfers to third countries so that, if it were faced today with a case involving facts similar to those in *Lindqvist*, it would likely be more hesitant to find that data transfer regulation does not apply to placing personal data on an Internet site.

Many third countries incorporate the standards of EU data protection law into their own law so that the conclusions of the CJEU in *Schrems* will reverberate around the world. By defining the standard that third countries must meet to be declared "adequate" as that of essential equivalence with EU law, the CJEU has set the global data protection bar at a high level.

Bradford has referred to the so-called "Brussels effect," in which the EU is engaged in unilateral regulation of global markets,[40] and which can be seen in the influence that EU data protection law has had on the development of data protection legislation in many third countries.[41] The *Schrems* judgment can be seen as an indirect example of the Brussels effect because it seems to be based on the rationale that withholding recognition of data transfers to the US may result in the US adopting standards closer to the European model.[42] The irony is that despite the criticisms that caused the CJEU to invalidate the Safe Harbour decision,

---

[37] *See* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 125–129 (2013).

[38] Case C-101/01, Bodil Lindqvist, 2003 E.C.R. I-12971.

[39] *See Schrems, supra* note 4, at para. 73.

[40] *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2013).

[41] *See* LEE BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 6215–16 (Kindle ed. 2014); Paul De Hert & Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 J. L. & POL'Y FOR INFO. SOC'Y 271, 287–88 (2013); Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68 (2012).

[42] *See* Popp, *supra* note 12 (including a statement by CJEU President, Koen Lenaerts, "[i]f this is also affecting some dealings internationally, why would Europe not be proud to contribute its requiring standards of respect of fundamental rights to the world in general?").

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

research into privacy compliance "on the ground" has found that EU law in general, and the Safe Harbour in particular, have played an important role in shaping how companies in the US process personal data.[43] Time will tell whether the new Privacy Shield will lead to further influence of EU data protection concepts on US practices.

III. The Role of the DPAs

By confirming that DPAs may not be precluded from examining the level of data protection in a third country set out in European Commission adequacy decisions, the CJEU substantially strengthened their role at the expense of the Commission. The judgment practically invites individuals to bring claims regarding the adequacy of protection in third countries to DPAs, who are then required to use "all due diligence" to examine them.[44] The DPAs are notoriously short on personnel and resources,[45] and evaluating the level of data protection in third countries can be a complicated exercise, so this new role will put a substantial burden on them.

There is tension between the encouragement the CJEU gave the DPAs in *Schrems* to use their powers under national law and the need for a more harmonized view of fundamental rights under the Charter. Article 25 of the Directive was intended to lead to a harmonized procedure for European Commission adequacy decisions,[46] but under the judgment, DPAs may take their own views of the adequacy of protection in third countries, though they may not themselves declare a decision illegal. In particular, the DPAs may use the powers granted to them by national law under Article 28 of the Directive, which the CJEU lists as "in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings."[47]

[43] *See* KENNETH BAMBERGER & DEIRDRE MULLIGAN, PRIVACY ON THE GROUND 65 (2015) (noting with regard to a survey of company privacy officers in the US that "respondents explained that European law plays a large role in shaping such company-wide privacy policies," and that "the influence of US law was evidenced by specific activities such as Safe Harbor certification").

[44] *See Schrems*, *supra* note 4, at para. 78.

[45] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES, (2010), http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.

[46] *See* SPIROS SIMITIS & ULRICH DAMMANN, EG-DATENSCHUTZRICHTLINIE 275 (1997).

[47] *Schrems*, *supra* note4, at para. 43.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

Under the GDPR, DPAs are also explicitly given the power to order the suspension of data flows to third countries.[48] This may result in a patchwork of different views among the DPAs and Member State courts on the level of protection in third countries, which effectively defeats the purpose of adequacy decisions by subjecting them to differing national interpretations and miring them in challenges to their validity.

At the same time, the CJEU has emphasized the need to take a more uniform view of fundamental rights under harmonizing measures such as the GDPR.[49] The consistency and cooperation mechanisms of the GDPR,[50] which require the DPAs to cooperate in the scope of the work of the new EU Data Protection Board—replacing the Article 29 Working Party—will also create pressure for the DPAs to adopt a more harmonized view of the adequacy of third countries. The DPAs will thus be caught between the CJEU's encouragement to make use of their enforcement powers on the one hand, and the need to adopt a harmonized interpretation of the standards for adequacy on the other hand.

IV. Defining an Adequate Level of Data Protection

The most controversial issue dealt with in the judgment is the CJEU's definition of an adequate level of protection for international data transfers under the Directive, which it defines as protection that is "essentially equivalent" but not necessarily "identical" to that under EU law. The standard that the CJEU adopts is best understood as a high degree of protection as determined by reference to the EU Charter of Fundamental Rights. At the same time, the allocation to the Member States of responsibility for national security presents the risk of gaps in the level of data protection, which should be addressed by the EU legislator and the CJEU.

1. The Charter as the Standard

The CJEU states several times in the *Schrems* judgment that the fundamental right to data protection is to be measured against the EU Charter of Fundamental Rights,[51] and makes frequent references both to the Charter and to previous judgments applying it, in particular

---

[48] *See* GDPR, *supra* note 3, art. 58(2)(j).

[49] *See* ECJ, Case C-399/11, Melloni v Ministerio Fiscal, ECLI:EU:C:2013:107, Judgment of 26 February 2013 (finding that when the EU legislator has harmonized fundamental rights protection in an exhaustive way, Member States are not allowed to "top up" fundamental rights protection).

[50] *See* GDPR, *supra* note 3, art. 60–76.

[51] *See*, *e.g.*, *Schrems*, *supra* note 4 at para. 38 (stating that "It should be recalled first of all that the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter"). *Id.* at para. 67 (stating that "It should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter").

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

Digital Rights Ireland. It also points out that the standard for an adequate level of protection is high,[52] and that the European Commission's review of requirements deriving from Article 25 of the Directive should be read strictly in light of the Charter.[53] The CJEU's case law also generally relies on the Charter in assessing fundamental rights.[54] Thus, the Charter is the measure for the regulation of international data transfers from the EU.

Under the Treaty on European Union (the "TEU"),[55] national security is the sole responsibility of each Member State. National security activities also fall outside the scope of the Directive and the GDPR.[56] The allocation of legislative competences in EU law, however, is not the same as the scope of application of the Charter.[57] The Charter applies to the Member States when they implement EU law,[58] and thus it applies to situations covered by the Directive as well—for example, when EU companies acting as data controllers transfer data to EU or third country intelligence services.[59] It also applies to many data protection situations involving national security, such as restrictions of data protection rights under Article 13(1)(a) of the Directive,[60] and to investigations regarding such restrictions by DPAs under Article 28(4) of the Directive.[61]

Nor does the fact that Article 4 TEU places competence for national security with the Member States necessarily mean that the Charter does not apply to the activities of third countries when they violate the fundamental rights of EU individuals. The territorial scope

---

[52] *Id.* at para. 39, 72, and 73.

[53] *Id.* at para. 78.

[54] Clara Rauchegger, *The Interplay Between the Charter and National Constitutions after* Åkerberg Fransson *and* Melloni, *in* THE EU CHARTER OF FUNDAMENTAL RIGHTS AS A BINDING INSTRUMENT 93, 122 (Sybe de Vries, Ulf Bernitz & Stephen Weatherill eds., 2015).

[55] Treaty on the Functioning of the European Union, *supra* note 19, at Article 4(2).

[56] Directive, *supra* note 2, art. 3(2)); GDPR, *supra* note 3, Recital 16.

[57] Rauchegger, *supra* note 54, at 97.

[58] Charter, *supra* note 20, art. 51(1). *See* Rauchegger, *supra* note 54, at 97.

[59] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU 11 (2015), http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf.

[60] Art. 13(1)(a) provides that "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard: (a) national security . . . ." Art. 23 of the GDPR, *supra* note 3, also allows restrictions to be put on data protection rights for national security reasons under strict conditions.

[61] Art. 28(4) provides in part that, "Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply."

of the Charter is the same as that of EU law,[62] and to the extent that EU law can apply to the activities of third country intelligence agencies, the Charter should as well.

The divergence between the level at which fundamental rights law is enacted—at the EU level—and that at which national security activities are carried out—by the Member States—risks producing gaps in protection. On the one hand, the Charter sets a high standard for the fundamental right of data protection, but on the other hand, national security activities are carried out by the Member States. In many situations involving data protection rights either EU law applies or there is an overlap between EU and Member State law, which results in application of EU law and thus, the application of the Charter. When EU law does not apply, such situations are governed solely by Member State constitutional law.[63] This could reduce the level of protection if data protection standards under Member State law are lower than those under the Charter. This risk is increased by the fact that it is often difficult to determine whether data are processed for national security purposes or not; for example, personal data may be collected or transferred for commercial or personal reasons but then may be accessed by national intelligence agencies and processed for national security purposes after the fact.[64]

It seems likely that the CJEU would take a restrictive view of claims that the Charter should not apply to data protection issues involving national security. Under Article 53, nothing in the Charter can be interpreted as adversely affecting human rights, and the constitutional autonomy of EU law, which the CJEU has taken pains to emphasize,[65] would not tolerate a lowering of the level of fundamental rights under the Charter based on the positions of some Member States or under a margin of discretion or appreciation based on the European Convention of Human Rights.[66] The official Explanations to the Charter prepared under the

---

[62] *See* Violeta Moreno-Lax & Cathryn Costello, *The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model*, *in* THE EU CHARTER OF FUNDAMENTAL RIGHTS, A COMMENTARY 1657 (Steve Peers, Tamara Harvey, Jeff Kenner, & Angela Ward eds., 2014).

[63] *See* Bruno de Witte, *Article 53—Level of Protection*, *in* THE EU CHARTER OF FUNDAMENTAL RIGHTS, A COMMENTARY, *supra* note 62, at 1527

> When a legal situation is outside the scope of EU law and within the scope of domestic law, there is no problem: Article 53 of the Charter simply confirms the evident rule that national constitutional rights will fully apply to such cases, notwithstanding any divergent formulation of those rights in the Charter.

[64] *See* Fred H. Cate, James X. Dempsey, & Ira S. Rubenstein, *Systematic Government Access to Private-Sector Data*, 2 INT'L DATA PRIVACY L. 195 (2012).

[65] *See* ECJ, Opinion 2/13, ECLI:EU:C:2014:2454, Opinion of 18 December 2014.

[66] *See* Koen Lenaerts & Jose Antonio Gutierrez-Fons, *The Place of the Charter in the EU Constitutional Edifice*, *in* THE EU CHARTER OF FUNDAMENTAL RIGHTS, A COMMENTARY, *supra* note 62, at 1581 (stating that "if the ECtHR ever decides

authority of the *Praesidium* of the Convention that drafted it also state that the Charter does not follow a "lowest common denominator" approach, and that Charter rights should be interpreted to offer a high standard of protection.[67] The Charter is intended to prevent a "race to the bottom" in fundamental rights standards,[68] such as could occur if low standards in certain Member States were taken as the measure for the fundamental right to data protection. Thus, allocation of legislative competence over national security to the Member States rather than the EU does not mean that they have unfettered discretion to interpret the concept of national security in order to remove their activities from scrutiny under EU fundamental rights law.[69]

The unclear delineation and definition of "national security" can produce confusion about the standards that should apply to Member State activities.[70] There is an urgent need for limitation or clarification of the meaning of the term in the context of data protection rights. Hopefully a case involving the allocation of national security to the Member States will reach the CJEU, in order to clarify the conditions under which the Charter applies to data protection issues that are affected by national security activities.

Following the *Schrems* judgment, some commentators (particularly those in the US) argued that it is hypocritical for EU policymakers and the CJEU to concern themselves with the standards of data protection for intelligence surveillance outside the EU, when the standards

---

to lower the level of protection below that guaranteed by EU law, by virtue of Article 53 of the Charter, the CJEU will be precluded from interpreting the provisions of the Charter in a regressive fashion").

[67] *See* Explanations Relating to the Charter of Fundamental Rights, 2007 O.J. (C 303) 17, 34.

[68] Rauchegger, *supra* note 54, at 125.

[69] *See* ECJ, Case C-300/11, ZZ v. Sec'y of State for the Home Dep't, ECLI:EU:C:2013:363, Judgment of 4 June 2014, para. 38 (holding that "the mere fact that a decision concerns State security cannot result in European Union law being inapplicable"). With regard to the related concepts of public policy and public security, see ECJ, Case C-348/09, P.I. v. Oberbürgermeisterin der Stadt Remscheid, EU:C:2012:300, Judgment of 22 May 2012, stating at paragraph 23 that:

> While Member States essentially retain the freedom to determine the requirements of public policy and public security in accordance with their national needs, which can vary from one Member State to another and from one era to another, particularly as justification for a derogation from the fundamental principle of free movement of persons, those requirements must nevertheless be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the institutions of the European Union.

See also HIELKE HIJMANS, THE EUROPEAN UNION AS GUARDIAN OF INTERNET PRIVACY 138–145 (2016).

[70] *See* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU, *supra* note 59, at 11.

that apply in the EU seem lacking in many respects.[71] In addition, there is widespread sharing of information by intelligence agencies of the Member States with the US, both under the "Five Eyes"[72] intelligence-sharing network (which includes Australia, Canada, New Zealand, the UK, and the US), and under bilateral arrangements involving Member States, such as France[73] and Germany.[74]

Strictly speaking, the data protection standards of Member State intelligence agencies are irrelevant for judging the standard of protection offered by third countries, and a violation of fundamental rights by a third country cannot be excused because Member State standards may be lacking. Yet, in a moral and political sense, the legitimacy of EU fundamental rights protection is undermined if the EU is viewed as holding third countries to standards that it is not willing to abide by itself. It would enhance the legitimacy of EU law in the eyes of third countries if national security was clearly brought within the ambit of EU fundamental rights law.

2. The Meaning of "Essentially Equivalent"

In the *Schrems* judgment, the CJEU explained that the standard of protection that third countries must meet under Article 25 of the Directive is one that is "essentially equivalent" to that under the Directive in light of the Charter.[75] It did so despite the fact that when the Directive was adopted, the EU legislator specifically preferred the term "adequate protection" over "equivalent protection."[76] The CJEU gave the following points of orientation to interpret the concept of essential equivalence (with parenthetical citations to the judgment): (1) There must be a high level of fundamental rights protection under the Charter and the CJEU's case law interpreting the Charter (paragraphs 38–39, 73), which

[71] *See*, *e.g.,* Geoffrey Robertson, *Opinion of Geoffrey Robertson QC for Facebook*, FIN. TIMES (Jan. 14, 2016), http://blogs.ft.com/brusselsblog/files/2016/01/Geoffrey-Robertson-QC.docx; SIDLEY AUSTIN LLP, *supra* note 11; *see also* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES, *supra* note 59; Stefan Heumann & Ben Scott, *Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany*, STIFTUNG NEUE VERANTWORTUNG (Sep. 30 2013), http://www.stiftung-nv.de/publikation/law-and-policy-internet-surveillance-programs-united-states-great-britain-and-germany (regarding oversight of intelligence surveillance in the Member States).

[72] *See* GLENN GREENWALD, NO PLACE TO HIDE 1581, 1854–1900 (Kindle ed. 2014) (regarding the Five Eyes alliance).

[73] *See* Vidya Root, *French Intelligence Involved in NSA Spying in France*, BLOOMBERG NEWS, (Nov. 29, 2013), http://www.bloomberg.com/news/articles/2013-11-29/french-intelligence-involved-in-nsa-spying-in-france-monde-says.

[74] *See Geheimdienst-Kooperation: BND leitet seit 2007 Daten an die NSA weiter*, SPIEGEL ONLINE, (Aug. 8, 2013), http://www.spiegel.de/netzwelt/netzpolitik/geheimdienste-bnd-leitet-seit-2007-daten-an-die-nsa-weiter-a-915589.html.

[75] *See Schrems*, *supra* note4, at para. 73.

[76] SIMITIS & DAMMANN, *supra* note 46, at 273.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

should be judged strictly (paragraph 78). (2) The third country in question must have a means for ensuring a high level of protection that is effective in practice (paragraph 74), in light of all the circumstances surrounding a transfer of personal data to a third country (paragraph 75). This must include periodic checks as to whether the adequacy assessment is still justified (paragraph 76) and take into account all circumstances that have arisen after adoption of the decision (paragraph 77). (3) Adequate protection must take into account the country's domestic law or international commitments (paragraph 71). (4) Any system of self-certification must be reliably based on effective detection and supervision mechanisms enabling infringements of the rules, in particular the right to respect for private life and the protection of personal data, to be identified and punished in practice (paragraph 81). (5) An adequacy decision must include a detailed explanation of how a country ensures an adequate level of protection (paragraph 83). (6) There must not be limitations based on national security, public interest, or law enforcement requirements that give third country law primacy over EU law (paragraphs 85–87). (7) Limitations must be placed on the power of public authorities (such as law enforcement authorities) to interfere with fundamental rights (paragraph 88). In particular, any such access must be strictly necessary and proportionate to the protection of values such as national security (paragraph 90), there must be clear and precise rules regarding the scope of application of a measure for effective protection against the risk of abuse of data (paragraph 91), and derogations and limitations in relation to data protection should apply only when strictly necessary (paragraph 92). (8) Third country legislation must not authorize, on a generalized basis, storage of all the personal data transferred without any differentiation, limitation, or exception being made in light of the objective pursued and without an objective criterion being laid down to determine the limits to the data, and its subsequent use, for purposes which are specific, strictly restricted, and capable of justifying the interference entailed by access to that data and its use (paragraph 93).

The term "essentially equivalent" seems to imply a comparison between third country data protection standards and EU standards, an undertaking that is fraught with difficulty. Data protection and privacy are "context-bound and linked to culture,"[77] making them difficult areas for comparative analysis. There are numerous theories used to compare different systems and concepts of constitutional and public law,[78] and selecting and refining the correct methodological approach in order to evaluate foreign legal systems of data protection is a lengthy and complex process. The European Commission has internal guidelines for evaluating the adequacy of the data protection law of third countries which

[77] Manuel José Cepeda Espinosa, *Privacy*, *in* THE OXFORD HANDBOOK OF COMPARATIVE CONSTITUTIONAL LAW 967 (Michel Rosenfeld & András Sajó, eds., Kindle ed. 2012). This is true even between the different EU Member States. *See* Marta Cartabia, *Europe and Rights: Taking Dialogue Seriously*, 5 EUR. CONST. L. REV. 5, 20 (2009).

[78] Vicki C. Jackson, *Comparative Constitutional Law: Methodologies*, *in* THE OXFORD HANDBOOK OF COMPARATIVE CONSTITUTIONAL LAW, *supra* note 77, at 54 (mentioning classificatory, historical, normative, functional, and contextual approaches).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

have never been made public, and the process of reaching an adequacy finding can take several years and involve participation by outside academic experts in foreign law. Comparison of legal systems is not a mechanical exercise—particularly in an area like data protection—and requires going beyond analysis of legal texts to consider factors such as constitutional protection, treaty protection, human rights institutions, civil law protection, criminal law, administrative law, and self-regulation.[79]

The *Schrems* judgment foresees DPAs being able to question European Commission adequacy decisions, and individuals being able to challenge them before national courts. One may be skeptical about how a DPA, with its limited resources, or a national court, with its focus on national or EU law, can conduct a meaningful comparison between third country law and EU data protection law. Because the determinations of national courts will generally be accepted by the CJEU without further inquiry if a reference for a preliminary ruling is sent to it,[80] there is a risk that the decision of whether essential equivalence exists could be made based on an insufficient evaluation of foreign law, such as when the evidence concerning foreign law is delivered only by a single party and is uncontested (as happened in the Irish proceeding that resulted the referral to the CJEU in *Schrems*[81]). In private international law scholarship, situations where evidence of foreign law is presented uncontested by a single party have been criticized as a "false application of foreign law,".[82] Intervention in references to the CJEU for a preliminary ruling is not possible,[83] meaning that there is no chance for third parties (such as foreign governments or academic experts) to provide further clarification on data protection standards in third countries. If the Court is going to deal increasingly with third country law, then its procedural rules should allow it to make an accurate evaluation of foreign law.

The fate of adequacy decisions will likely depend to a large extent on the record in the national cases that are referred to the CJEU for a decision. This makes it important for third countries to monitor proceedings in national courts regarding the validity of adequacy decisions concerning them and to attempt to intervene in such proceedings at the national level when possible, because all parties to the main proceedings at the national level may

[79] *See* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS 53 (2014).

[80] *See* KOEN LENAERTS, IGNACE MASELIS, & KATHLEEN GUTMAN, EU PROCEDURAL LAW 15562 (Kindle ed. 2014) (noting that "under settled case-law, in the context of preliminary ruling proceedings, the Court of Justice is not entitled to rule on facts or points of national law, or to verify whether they are correct").

[81] *See* Schrems v. Data Prot. Comm'r, [2014] 2 I.L.R.M. 441 (H. Ct.) (Ir.), [2014] I.E.H.C. 310.

[82] *See* M. Jänterä-Jareborg, *Foreign Law in National Courts: A Comparative Perspective*, 304 RECUEIL DES COURS/COLLECTED COURSES OF THE HAGUE ACAD. OF INT'L L. 181, 233 (2003).

[83] *See* LENAERTS, MASELIS, & GUTMAN, *supra* note 80, at 23573.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

then participate in the procedure before the CJEU.[84] The CJEU could also consider ordering measures of inquiry, such as expert reports, pursuant to its Rules of Procedure, which is permitted in a preliminary ruling on the validity of an EU act.[85]

By finding that adequacy requires essential equivalence with EU law, the CJEU's intention seems to have been to emphasize that the level of protection that third countries offer must be high and come close to that under EU law, without being absolutely identical. This could well have been expressed in other terms with the same meaning, such as by saying that third countries "must meet a high standard of protection under the Charter" or something similar. Thus, examining the data protection standards required by the Charter and its interpretation in cases like *Digital Rights Ireland* and *Schrems* is more likely to lead to a meaningful understanding of the standard the CJEU requires than is merely parsing the linguistic meaning of the terms "essentially" and "equivalent."

3. The EU-US Privacy Shield and the GDPR

An evaluation of the voluminous documentation that comprises the Privacy Shield would exceed the scope of this article.[86] Rather, the focus will be on its implications for EU regulation of international data transfers.

The basic construction of the Privacy Shield is similar to that of the Safe Harbour, in that it is based on a set of principles derived from EU data protection law that companies can voluntarily self-certify to, and compliance with which is policed by the FTC and DOT. The substance of the Privacy Shield includes both primary[87] and supplemental principles[88] that are close to those of the Safe Harbour, but are generally more detailed. In contrast with the

[84] *See id*. In Schrems II 2016/4809 P, the Irish High Court has allowed interventions by the US government and other external stakeholders. *See* Irish High Court, Judgment of Mr. Justice McGovern, 19 July 2016, https://regmedia.co.uk/2016/07/19/facebook_eff_schrems.pdf.

[85] *See* Lenaerts, Maselis, and Gutman, *supra* note 80, at 19002–015 (noting that "it would be perfectly possible for measures of inquiry to be ordered pursuant to art. 64(2) of the ECJ Rules of Procedure"). Art 64(2) foresees such measures as "the commissioning of an expert's report".

[86] The complete documentation of the Privacy Shield can be found at http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm and https://www.privacyshield.gov/EU-US-Framework.

[87] The principles include Notice, Choice, Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse Enforcement and Liability.

[88] These include Sensitive Data; Journalistic Exceptions; Secondary Liability; Performing Due Diligence and Conducting Audits; The Role of the Data Protection Authorities; Self-Certification; Verification; Access; Human Resources Data; Obligatory Contract for Onward Transfers; Dispute Resolution and Enforcement; Choice—Timing of Opt Out; Travel Information; Pharmaceutical and Medical Products; Public Record and Publicly Available Information; and Access Requests by Public Authorities.

Safe Harbour, the Privacy Shield also includes commitments from US national security officials concerning protections given to data from EU citizens, as well as letters and statements from other US government officials.

The negotiations between the EU and the US were marked by secrecy, and there was political pressure to have the Privacy Shield enacted as quickly as possible.[89] Both the Article 29 Working Party and the European Data Protection Supervisor (EDPS) have expressed doubts about its compatibility with EU data protection standards.[90] US President Trump has also stated that he will repeal all of the executive orders issued by former President Obama,[91] some of which form an essential element of the Privacy Shield.[92] All these factors suggest that the Privacy Shield may have an uncertain fate before the CJEU.

The application of the GDPR will also present challenges for the Privacy Shield. The GDPR includes a detailed definition of what constitutes "adequacy" for data transfers to third countries that incorporates the standards adopted by the CJEU in *Schrems*.[93] The GDPR is much more complex than the Directive under which *Schrems* was decided, and includes rules in a number of areas that are not covered in the Privacy Shield.[94] This suggests that the Privacy Shield may have to be substantially amended in order to continue to provide protection that is "essentially equivalent" once the GDPR comes into force. The European Commission seems to realize this because it has promised to suspend the Privacy Shield as

[89] *See*, *e.g.,* Zoya Sheftalovich, *5 Takeaways from the Privacy Shield*, POLITICO, Feb. 29, 2016, http://www.politico.eu/article/privacy-shield-agreement-takeaways-text-released/ (stating that "the Council's biggest concern is how quickly the new arrangement can be up and running").

[90] ARTICLE 29 WORKING PARTY, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, WP 238 (Apr. 13, 2016); European Data Protection Supervisor, Opinion on the EU-U.S. Privacy Shield Draft Adequacy Decision, Opinion 4/2016, (May 30, 2016).

[91] *See* Donald J. Trump, Remarks at a Rally at the Greenville Convention Center in Greenville, North Carolina (Sept 6, 2016), http://www.presidency.ucsb.edu/ws/?pid=119197, (including Trump's statement that "we are going to eliminate every unconstitutional executive order and restore the rule of law to our land").

[92] *See* Commission Implementing Decision 2016/1250, *supra* note 13 (emphasizing in Recitals 68–69 the importance of US Presidential Policy Directive 28 of 17 January 2014 for the Privacy Shield).

[93] *See* GDPR, *supra* note 3, art. 45(2).

[94] For example, concerning the use of data protection impact assessments (art. 35 GDPR); data portability (art. 20 GDPR); and data protection by design and by default (art. 25 GDPR).

of the date of application of the GDPR[95] and to assess the level of protection provided by the Privacy Shield at that time.[96]

D. The Effect of *Schrems* on Other Data Transfer Mechanisms

I. Introduction

The rule of law requires the consistent application of legal rules to similar situations,[97] and the CJEU strives to ensure that its judgments enjoy legitimacy based on criteria such as coherency with existing case law, predictability, and avoidance of arbitrariness.[98] It is therefore important to look beyond the Safe Harbour and investigate the implications of the *Schrems* judgment for the other legal bases for data transfers under the Directive, particularly because the legality of one of them (the standard contractual clauses) is at issue in the *Schrems II* case currently before the Irish courts.[99]

There are three legal bases for international data transfers mentioned in the Directive, namely adequacy decisions issued by the European Commission (Article 25), "adequate safeguards" (Article 26(2), known as "appropriate safeguards" under the GDPR[100]), and derogations (Article 26(1)), the standards for which all differ. The GDPR retains all three of these legal bases.

As clarified by the CJEU in *Schrems*, an adequacy decision requires that the legal system of a third country be "essentially equivalent" to that of EU data protection law, which represents the highest standard. When there is no adequacy in the third country to which data are to be transferred, adequate safeguards may be used. Such safeguards are based not on a detailed evaluation of the legal system of the country to which the data are to be transferred

---

[95] *See* Commission Implementing Decision (EU) 2016/1250, *supra* note 13, note 208 (stating:

> As of the date of application of the General Data Protection Regulation, the Commission *will make use of its powers* to adopt, on duly justified imperative grounds of urgency, *an implementing act suspending the present decision* which shall apply immediately without its prior submission to the relevant comitology committee and shall remain in force for a period not exceeding six months.

(emphasis added)).

[96] *See id.* Recital 146.

[97] *See* GUNNAR BECK, THE LEGAL REASONING OF THE COURT OF JUSTICE OF THE EU 234 (Kindle ed. 2012).

[98] *See* Koen Lenaerts, *How the ECJ Thinks: A Study on Judicial Legitimacy*, 36 FORDHAM INT'L L. J. 1302, 1306 (2013).

[99] *See* Schrems II, *supra* note 21.

[100] *See* GDPR, *supra* note 3, art. 46.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

as is the case in an adequacy decision, but are a set of protections that apply to the particular data transfer. They can be seen as the middle level of protection. Finally, derogations, by definition, may apply when there is no essential equivalence nor appropriate safeguards that can be used.[101] In such a case, there may not be any protection in place, which makes derogations the lowest standard.

In theory, the difference in standards between the three sets of legal bases for data transfers means that one may be invalid without affecting the others. For example, the fact that an adequacy decision is invalid for not providing essential equivalence (the highest standard) does not mean that a transfer may not be possible based on adequate safeguards (the middle standard). Yet, if criticism of an adequacy decision can be applied by analogy to other legal bases for data transfer, or if data gathering practices that result in invalidation of an adequacy decision also violate the standards of these other bases, then this would seem to raise questions about their continued viability as well.

II. Commission Adequacy Decisions

Article 25 of the Directive provides that transfers of personal data require that the third country provide an adequate level of data protection. The most prominent method of ensuring adequate protection is via a formal adequacy decision of the European Commission, of which the Safe Harbour was an example.[102] The *Schrems* judgment is based on a strict interpretation of the standards of data protection in third countries, and on a strong emphasis on the protection of data protection rights when transferring data internationally.[103] These criteria must be applied to other adequacy decisions as well.

The same points made by the CJEU concerning access to data by the US intelligence services could be raised concerning several other adequacy decisions. Two of the countries that

[101] *See* Directive 95/46, *supra* note 2, art. 26(1) (providing that the derogations provide a legal basis for data transfers to a third country "which does not ensure an adequate level of protection within the meaning of Article 25(2)").

[102] There are currently thirteen European Commission adequacy decisions in force, covering Andorra; Argentina; the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA); Switzerland; the Faroe Islands; Guernsey; Israel; the Isle of Man; Jersey; New Zealand; the EU-US Privacy Shield; Uruguay; and transfers of passenger name records of air passengers transferred to the Canada Border Services Agency. In January 2017, the Commission announced that it will "actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017, and, depending on progress towards the modernisation of its data protection laws, with India, but also with countries in Latin America, in particular Mercosur, and the European neighbourhood which have expressed an interest in obtaining an 'adequacy finding.'" *See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World*, at 8, COM (2017) 7 final, (Jan. 10, 2017).

[103] *See*, *e.g.*, *Schrems*, *supra* note4, at para. 78 (stating that "review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict").

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

participate in the international "Five Eyes" intelligence sharing network have also been found adequate, namely Canada[104] and New Zealand.[105] The judgment in *Schrems* is based on findings of the Irish High Court that US surveillance programs revealed "the large scale collection and processing of personal data";[106] that there was a "'significant over-reach' on the part of the NSA and other federal agencies";[107] and that in the US there has been "indiscriminate surveillance and interception carried out by them on a large scale."[108] In light of these findings, it seems unclear how countries such as those that are part of the Five Eyes network and have deep and longstanding intelligence-sharing arrangements with the US can provide a level of data protection that is "essentially equivalent" to the protection provided by EU law. This question could also be asked of Israel, which has been found adequate despite having a longstanding tradition of intelligence cooperation with the US.[109]

III. Adequate Safeguards

Article 26(2) of the Directive provides that transfers may be carried out absent adequate protection in the third country to which personal data are transferred "where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses." The GDPR maintains the concept of adequate safeguards, which it refers to as "appropriate safeguards," and adds a number of conditions to their use.[110]

Under the Directive and the GDPR, two main types of "adequate safeguards" are recognized, namely contractual clauses and binding corporate rules (BCRs). Contractual clauses are

[104] *See* Commission Decision 2002/2 of 20 December 2001 Pursuant to Directive (EC) 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, 2002 O.J. (L 2) 13 (EC); Commission Decision of 6 September 2005 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the Canada Border Services Agency, 2005 O.J. (L 91) 49.

[105] *See* Commission Implementing Decision of 19 December 2012 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by New Zealand, 2013 O.J. (L 28) 12.

[106] *See Schrems*, *supra* note 4, at para. 11.

[107] *Id.* at para. 30.

[108] *Id*. at para. 31.

[109] Commission Decision 2011/61 of 31 January 2011 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the State of Israel with Regard to Automated Processing of Personal Data, 2011 O.J. (L 27) 39 (EU). *See* GREENWALD, *supra* note 72, at 1904 (stating that "the NSA has a surveillance relationship with Israel that often entails cooperation as close as the Five Eyes partnership, if not sometimes even closer").

[110] *See* GDPR, *supra* note 3, art. 46–47.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

concluded between the data exporter in the EU and the data importer outside the EU to whom the data are sent, and contain obligations on each to provide certain protections to the personal data. They can either be "standard contractual clauses," the text of which is standardized and adopted by a formal decision of the European Commission,[111] or *ad hoc* clauses that are drafted in each specific case and may need to be approved by the DPAs before use.[112] BCRs are legally-binding internal codes that are adopted by a corporate group and approved by DPAs, and provide a legal framework for data transfers within the group or to it.[113] The standard for what constitutes adequate safeguards has been set forth in the detailed guidance that has been issued by the European Commission and the Article 29 Working Party concerning standard contractual clauses and BCRs—for example, the European Commission decisions recognizing standard clauses[114] and the Article 29 Working Party's opinions on both these methods of transfer.[115]

Adequate safeguards were not at issue in the *Schrems* case, so that in a formal legal sense the judgment did not affect them. A Communication issued by the European Commission in November 2015 emphasized that following the judgment other data transfer mechanisms under the Directive may still be used, such as derogations, for example consent under Article 26(1) of the Directive, and adequate safeguards, for example BCRs or standard contractual clauses under Article 26(2).[116] As stated above, a case is currently pending before the Irish courts that is likely to be referred to the CJEU concerning the validity of the standard contractual clauses.[117]

Despite their continued validity in a formal legal sense, adequate safeguards are just as unable to protect against intelligence surveillance as are adequacy decisions. It is clear that a contractual agreement between two private parties, or a binding set of data protection rules within a corporate group, cannot legally restrain government intelligence activities of

---

[111] *See* EUROPEAN COMMISSION, MODEL CONTRACTS FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[112] *See* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 191–208 (2d ed. 2007) (regarding the use of contractual clauses to transfer data). The GDPR deals with contractual clauses in art. 46.

[113] *See* LOKKE MOEREL, BINDING CORPORATE RULES: CORPORATE SELF-REGULATION OF GLOBAL DATA TRANSFERS (2012) (regarding BCRs).

[114] *See* Model Contracts for the Transfer of Personal Data to Third Countries, *supra* note 111.

[115] *See* European Commission, Opinions and Recommendations, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[116] *See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America Under Directive 95/46/EC Following the Judgment by the Court of Justice in Case C-362/14 (Schrems),* COM (2015) 566 final, (Nov. 6, 2015).

[117] *See* Schrems II, *supra* note 21.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

third countries. Moreover, in a practical sense, the powers of intelligence services to access data far exceed any protections that can be granted by contracts or corporate compliance policies. Decisions by the European Commission and opinions by the Article 29 Working Party on standard contractual clauses and BCRs also make it clear that adequate safeguards cannot allow data access by law enforcement and intelligence agencies of third countries that goes beyond what is necessary in a democratic society and has a substantial adverse effect on the guarantees provided by applicable data protection law.[118]

In his submission to the CJEU, Schrems implied that the use of the standard contractual clauses results in a higher level of protection than does an adequacy decision like Safe Harbour, because transfers under the clauses are "under supervision by DPAs."[119] Yet, not all Member States require that the standard clauses be filed with the DPAs,[120] and under the GDPR, the use of the standard clauses adopted by the Commission or by a DPA does not require DPA authorization.[121] In addition, under the Directive, the DPAs' statutory enforcement powers end at their national borders.[122] While the standard contractual clauses do include provisions giving the DPAs rights with regard to data importers,[123] they cannot allow the DPAs to exercise their statutory powers in third countries. Thus, the argument that the use of adequate safeguards provides added protection because of DPA involvement is essentially a legal fiction.

The conclusions of the CJEU in *Schrems* have thus undermined the logical consistency of using adequate safeguards to transfer personal data. The European Commission and the DPAs have allowed standard contractual clauses and BCRs to be used for years although it has been clear that they cannot provide effective protection against intelligence surveillance, suggesting that until now they have implicitly factored the possibility of such

---

[118] *See*, *e.g.,* Commission Decision 2010/87 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 O.J. (L 39) 5, art. 4(1)(a) (EC); ARTICLE 29 WORKING PARTY, *Explanatory Document on Processor Binding Corporate Rules*, WP 204 rev.01, (May 22, 2015) at 13.

[119] *See* Schrems v. Data Prot. Comm'r, *Written Submissions of Applicant*, EUROPE VERSUS FACEBOOK 24 http://www.europe-v-facebook.org/CJEU_subs.pdf.

[120] *See* ARTICLE 29 WORKING PARTY, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual Clauses" Considered as Compliant with the EC Model Clauses*, WP 226, (Nov. 24, 2014), at 2, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf.

[121] *See* GDPR, *supra* note 3, art. 46(2).

[122] *See* EU Data Protection Directive, *supra* note 2, art. 28(6). *See also* ECJ, Case C-230/14, Weltimmo, ECLI:EU:C:2015:639, Judgment of 1 October 2015, para. 60.

[123] *See, e.g.*, Commission Decision 2010/87 of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors, *supra* note 118, Clause 8, (EC) (giving DPAs the right to conduct an audit of the data importer).

surveillance into the definition of "adequate safeguards." The strict standard for data protection rights applied by the CJEU in *Schrems* judgments raises the question of whether this is compatible with EU fundamental rights law.

IV. Derogations

Article 26(1) of the Directive includes derogations to the restrictions on data transfers to third countries. The derogations are meant to cover situations in which there is no adequate protection in the country of data transfer, but "[t]he risks to the data subject are relatively small" or "[o]ther interests (public interests or those of the data subject himself) override the data subject's right to privacy."[124] They are to be narrowly construed,[125] and cannot generally provide a long-term framework for "repeated or structural data transfers."[126]

Under the Directive, these derogations apply in the following situations: "The data subject has given his consent unambiguously to the proposed transfer" (26(1)(a)); or "the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request" (26(1)(b)); or "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party" (26(1)(c)); or "the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims" (26(1)(d)); or "the transfer is necessary in order to protect the vital interests of the data subject" (26(1)(e)); or "[T]he transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case" (26(1)(f)). The GDPR maintains these derogations, and also allows data transfers under certain narrow circumstances based on the compelling legitimate interests of the data controller.[127]

As is the case with appropriate safeguards, the use of derogations was not at issue in the *Schrems* judgment. Because the derogations are designed for situations where no adequate protection exists or no adequate safeguards can be used, their use is not directly affected by *Schrems*, as long as the conditions for application of the derogations are observed, i.e., they must be narrowly construed and not used for repeated or structural data transfers, and

[124] ARTICLE 29 WORKING PARTY, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, WP 12, (July 24, 1998) at 24.

[125] *See id*.

[126] ARTICLE 29 WORKING PARTY, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, (Nov 25, 2005) at 11 (regarding consent).

[127] *See* GDPR, *supra* note 3, art. 49(1).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

as derogations from a fundamental right must be interpreted strictly.[128] Since by definition derogations do not provide any protection, they cannot guard against intelligence surveillance such as was at issue in *Schrems*.

E. Conclusions

I. Data Transfer Regulation Between Reality and Illusion

The *Schrems* judgment demonstrates both the reality and the illusion of the regulation of international data transfers under EU data protection law. The CJEU's strong affirmation of the application of the Charter to international data transfers continues the reality of legal protection for data protection rights that was advanced in *Digital Rights Ireland* and other judgments.

At the same time, it shows how EU law maintains the "exalting illusion" of imagining that EU standards can protect data transfers on a global basis. The points upon which the CJEU relied to invalidate the Safe Harbour can be applied analogously to other legal mechanisms for data transfers under the Directive as well, and the system the judgment sets up for having adequacy decisions evaluated at the national level will be difficult to implement in practice. While the Charter provides the measure of adequate protection for data transfers in most cases, the exemption of national security from EU competence causes gaps in protection. The judgment thus lays bare the internal contradictions of the regulation of data transfers under EU law, and shows how its unilateral application cannot provide complete protection for data transfers to third countries. This is illustrated by the fact that despite the CJEU's strong affirmation of data protection rights in the judgment, little enforcement action was taken[129] in the period between the invalidation of the Safe Harbour and the entry into force of the Privacy Shield. Such a failure of enforcement can only lead to a lack of respect for data protection law.[130]

---

[128] *See*, *e.g.,* Digital Rights Ireland & Seitlinger, *supra* note 30, para. 52; *see also* PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW 532, 670 (4th ed. 2008); TAKIS TRIDIMAS, THE GENERAL PRINCIPLES OF EU LAW 209 (2d ed. 2009).

[129] *See*, *e.g.,* Julia Fioretti, *German Privacy Regulator Fines Three Firms over U.S. Data Transfers*, REUTERS (June 6, 2016), http://www.reuters.com/article/us-germany-dataprotection-usa-idUSKCN0YS23H (describing how the DPA of the German state of Hamburg fined three US companies for continuing to rely on the Safe Harbour after the *Schrems* judgment was issued); *see also* ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14, (Oct. 14, 2015), 4 https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf (showing the data protection authority of the German federal state of Schleswig-Holstein's statement that, "In consistent application of the requirements explicated by the CJEU in its judgment, a data transfer on the basis of Standard Contractual Clauses to the US is no longer permitted").

[130] *See* CHRIS REED, MAKING LAWS FOR CYBERSPACE 49 (2012).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

II. Bureaucracy and Formalism in Data Transfer Regulation

The regulation of international data transfers relies heavily on bureaucratic, formalistic measures, including the signature of contractual clauses, consent clauses in online forms, lengthy processes for the approval of BCRs by DPAs, filings of forms with DPAs where companies provide information about their data processing and data transfer practices, and other similar mechanisms. The procedure for having third countries declared "adequate" by the European Commission is also a triumph of bureaucracy and formalism over substance, and has been criticized as inefficient,[131] untransparent,[132] and subject to political influence.[133] The inefficiency of the process is demonstrated by the low number of adequacy decisions issued since the Directive came into effect in 1998. There are only thirteen data protection adequacy decisions currently in force, but by contrast the European Commission has made well over 100 decisions in the last few years finding third country legal regimes equivalent to EU rules in areas of financial services regulation such as accounting standards, statutory audits, and the operation of credit rating agencies.[134] While the slow pace of adopting adequacy decisions in data protection may partly reflect the wide variety of approaches to data privacy around the world and the difficulty of comparing different systems of fundamental rights, it may also be caused, at least in part, by the opacity and poorly defined nature of the process.

Like any fundamental right, data protection cannot be reduced to a set of formalistic or bureaucratic procedures. The CJEU in *Schrems* emphasized that protections provided for personal data transferred from the EU to third countries must "prove, *in practice, effective* in order to ensure protection essentially equivalent to that guaranteed within the European

[131] *See* ARTICLE 29 WORKING PARTY, *The Future of Privacy* WP 168 (Dec. 1, 2009), at 10–11 (regarding problems with the EU system for reaching adequacy determinations and stating that the process for reaching adequacy decisions should be "redesigned").

[132] *See* KUNER, *supra* note 37, at 48.

[133] For example, in July 2010 the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports. *See* John Ihle, *Ireland Blocks EU Data Sharing with Israel*, JTA (July 8, 2010), http://www.jta.org/2010/07/08/news-opinion/world/ireland-blocks-eu-data-sharing-with-israel. Israel later received an adequacy decision from the European Commission. *See* Commission Decision 2011/61 of 31 January 2011, *supra* note 109. *See also* Jennifer Stoddart, Benny Chan, & Yann Joly, *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research*, 44 J. L. MED. & ETHICS 143 (2016) (criticizing the consistency of European Commission adequacy decisions).

[134] For the current status of Commission decisions concerning equivalence of foreign frameworks in the area of banking and finance, *see* http://ec.europa.eu/finance/general-policy/global/equivalence/index_en.htm. *See* Tzung-bor Wei, *The Equivalence Approach to Securities Regulation*, 27 NW. J. INT'L L. & BUS. 255 (2006) (regarding the concept of "equivalence" in securities regulation).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

Union (emphasis added)."[135] Both the European Court of Human Rights[136] and the Article 29 Working Party[137] require that remedies for data protection violations be effective in practice as well as in law. Individuals in the EU whose data are transferred internationally are also interested in ensuring that their rights are protected in practice, as is indicated by the widespread concern among Europeans about the misuse of their data online.[138]

Access to personal data transferred under Safe Harbour by the US intelligence services was one of the main factors underlying the *Schrems* judgment, which can be seen in the CJEU's criticism that the Safe Harbour principles can be limited by national security or law enforcement requirements,[139] the lack of limits on data use under US law for national security purposes,[140] and the Safe Harbour's failure to contain any legal protection dealing with US intelligence surveillance.[141] In light of this, one can only conclude that the judgment requires meaningful and effective protection against intelligence surveillance by third countries. Procedures such as checking consent boxes on online forms, signing contractual clauses, or having BCRs approved by DPAs cannot restrain data access by foreign intelligence services. At a legal level, EU law does not constrain the actions of the public authorities and agencies of third countries, and at a practical level, their capabilities are not in any way hindered by such procedural mechanisms.

The Privacy Shield contains a number of paper-based, formalistic requirements, such as submitting a detailed self-certification statement annually to the US Department of Commerce,[142] developing and publishing a privacy policy statement,[143] and filing a

---

[135] *See* Schrems, *supra* note 4, at para. 74; *id.* at para. 39 (referring to the need for "effective and complete" protection); *id.* at para. 41 (referring to the importance of ensuring the "effectiveness" of monitoring of compliance with the law by DPAs); *id.* at para. 81, 89, 91, 95 (stressing the need for protection of the fundamental right to data protection to be "effective").

[136] *See*, *e.g.*, Rotaru v. Romania 2000 Eur. Ct. H.R. 191, para. 67.

[137] *See* ART. 29 WORKING PARTY, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* WP 12 (July 24, 1998), at 5 (stating that "data protection rules only contribute to the protection of individuals if they are followed in practice").

[138] *See* Directorate-General for Communication, *Special Eurobarometer 431: Data Protection*, 25 (June 2015), http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf.

[139] *See* Schrems, *supra* note 4, at para. 84–86.

[140] *Id.* at para. 88.

[141] *Id.* at para. 89.

[142] *See Self-Certification*, EXPORT.GOV, PRIVACY SHIELD PROGRAM (July 6, 2016) https://www.export.gov/article?id=6-Self-Certification.

[143] *See How to Join Privacy Shield (Part 1)*, EXPORT.GOV, PRIVACY SHIELD PROGRAM (Apr. 13, 2017), https://www.export.gov/article?id=How-to-Join-Privacy-Shield-part-1.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

registration with an independent recourse mechanism.[144] Some elements of the Privacy Shield do seem to offer hope of more effective protection against data access by law enforcement and intelligence authorities, such as a detailed annual joint review of the Privacy Shield by the European Commission, DPAs, and various US government agencies,[145] and the establishment by the US of a Privacy Shield Ombudsperson to deal with questions relating to oversight of national security authorities.[146] The proposed Umbrella Agreement[147] and changes to US legislation[148] also seem to be steps in the right direction, and could provide additional legal support to the Privacy Shield.

It will take several years before the CJEU has a chance to opine on the Privacy Shield, so that there is a window of opportunity to determine how it works in practice. Unless one is unalterably opposed to resolving questions concerning international data transfers through cooperation between legal systems, it seems worthwhile to give the Privacy Shield a chance to prove itself. If it does lead to a higher level of protection in practice, then it deserves to survive; if not, then it will no doubt suffer the same fate as the Safe Harbour.

III. Data Localization

The *Schrems* judgment has provoked interest in what can be described as data localization, meaning measures or policies to encourage or require the storage of personal data inside the borders of the EU.[149] Incentives have been proposed to store the data of European companies on servers located within the EU,[150] and a number of US-based companies have announced plans to store data in Europe.[151] The CJEU has also hinted that fundamental

---

[144] *See How to Join Privacy Shield (Part 2)*, EXPORT.GOV, PRIVACY SHIELD PROGRAM (Apr. 13, 2017) https://www.export.gov/article?id=How-to-Join-Privacy-Shield-part-2.

[145] *See* Commission Implementing Decision 2016/1250 of 12 July 2016, *supra* note 13, Recitals 147–48.

[146] *Id.* Recital 65.

[147] *See* Agreement on the Protection of Personal Information, *supra* note 15.

[148] *See* Judicial Redress Act of 2015, *supra* note 17.

[149] *See* Anupam Chander & Uyê P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015) (regarding data localization); Christopher Kuner, *Data Nationalism and its Discontents*, 64 EMORY L.J. ONLINE 2089 (2015), http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf.

[150] *See Atos CEO Calls for 'Schengen for Data,'* THIERRY BRETON'S BLOG, http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html; *Ein Internet nur für Deutschland*, FRANKFURTER ALLGEMEINE ZEITUNG, (Nov. 10, 2013), http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html.

[151] *See Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America*, *supra* note 116, at 12; *see also* Murad Ahmed & Richard Waters, *Microsoft Unveils German Data Plan to Tackle US Internet Spying*, FIN. TIMES, (Nov. 11, 2015) http://www.ft.com/intl/cms/s/0/540a296e-87ff-11e5-9f8c-a8d619fa707c.html#axzz3vvmkIE7x; Karlin Lillington,

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

rights law may require the storage of personal data within the boundaries of the EU in certain circumstances.[152] The question is whether data localization can provide complete protection against data access by the intelligence services; the answer seems to be "no."

It is obvious that not all data processing services can be located in the EU. Thus, using data localization to avoid data transfers to third countries may help in isolated cases, but cannot be a large-scale solution. From the popularity of Internet services,[153] it is clear that Europeans want to communicate with parties in third countries and exchange data with them. Under both EU and international human rights law, individuals have a right to communicate and transfer data "regardless of frontiers,"[154] suggesting that the ability to communicate across national borders is a necessary component of the right to freedom of expression.[155]

Storing data on computers physically located in the EU Member States removes them from the direct enforcement jurisdiction of third countries because under international law public authorities may generally not enforce laws abroad without the consent of the country where enforcement is to be carried out.[156] It may also be easier for EU individuals to assert their data protection rights with regard to data stored in the EU, because EU law provides a framework for the assertion of rights by parties located in different Member States.[157]

Oracle Keeps European Data Within Its EU-Based Data Centres, IR. TIMES, (Oct. 28, 2015), http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot; Paul M. Schwartz & Karl-Nikolaus Peifer, *Datentreuhändermodelle – Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte*?, 3 COMPUTER UND RECHT 165 (2017).

[152] *See* ECJ, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB & Sec'y of State for the Home Dep't, ECLI:EU:C:2016:970, Judgment of 21 December 2016, at para. 114.

[153] For example, as of June 2015, 57% of Europeans use an online social network at least once a week, and 53% use instant messaging or chat websites. *See* Directorate-General for Communication, *Special Eurobarometer 431: Data Protection*, 24 (June 2015), http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf.

[154] *See* Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III), Dec. 10, 1948, art. 19; International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Exec. Rep. 102-23, 999 U.N.T.S. 171, Article 19(2); European Convention for the Protection of Human Rights and Fundamental Freedoms, Sept. 3, 1953, E.T.S. 5, 213 U.N.T.S. 221, Article 10(1).

[155] In each of the three human rights conventions referred to above in note 154, the phrase "regardless of frontiers" is mentioned in the article dealing with freedom of opinion and of expression (for example, in the articles cited therein).

[156] *See*, *e.g.*, IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 309 (7th ed. 2008).

[157] *See*, *e.g.*, EU Data Protection Directive, *supra* note 2, art. 28(6) (obliging EU DPAs to cooperate with each other); Council Regulation 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 2001 O.J. (L 12) 1 (EC).

However, as the Snowden revelations have shown, there is widespread data sharing between EU intelligence services and those of third countries, in particular the US services and those of the "Five Eyes" intelligence sharing network.[158] It seems that the cooperation between the US National Security Agency (NSA) and the UK signals intelligence service Government Communication Headquarters (GCHQ) is particularly close.[159] This suggests that data sharing is being conducted on a broad scale between intelligence agencies in many countries, and that once data are accessed by one agency, they may be made available to those in other countries, so that the place of the computer where data are stored may be largely irrelevant to whether they can be accessed by the intelligence services. It is also not clear that the place of data storage affects the technical capabilities of intelligence services of third countries to access data stored in the EU, given the global and networked nature of data processing. Thus, the available evidence gives reason to doubt that the place of data storage has much influence in practice on the level of protection that personal data receives.

IV. The Politics of International Data Transfers

The political nature of the regulation of international data transfers can be seen particularly in the relationship between the EU and the US. Parties in the EU want the US to adopt an EU-style data protection framework,[160] while for its part the US side would like the EU to make it easier to transfer personal data internationally, both to further economic growth[161]

---

[158] *See*, *e.g.,* GREENWALD, *supra* note 72, at 1852–1926 (stating that there is a wide-ranging intelligence sharing network between US intelligence agencies such as the National Security Agency (NSA) and those of other countries, including both the Five Eyes countries and others such as Israel); Maik Baumgärtner et al., *Spying Close to Home: German Intelligence under Fire for NSA Cooperation*, SPIEGEL ONLINE (Apr. 24, 2015), http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html (criticizing cooperation between the German intelligence services and those of the US); Julian Border, *GCHQ and European Spy Agencies Worked Together on Mass Surveillance*, THE GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden, (alleging close cooperation between the British, French, German, Spanish, and Swedish intelligence agencies).

[159] *See* GREENWALD, *supra* note 72, at 1857 (stating that the GCHQ is the "closest NSA ally"); Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,* 56 HARV. INT'L L. REV. 81, 126 (2015).

[160] *See*, *e.g.*, Press Release, Transatlantic Consumer Dialogue (TACD), Transatlantic Consumer Dialogue (TACD) Organization Calls on US to Enact Privacy Legislation to Ensure Fundamental Rights, http://tacd.org/wp-content/uploads/2015/10/TACD-Statement-in-response-to-the-European-Court-of-Justice-ruling-on-Safe-Harbor-agreement-.pdf (stating that "It is also more than high time for the United States to enact a comprehensive set of data protection rules, to bring it in line with 100 plus other countries round the world"). The TACD includes numerous consumer organizations in both the EU and the US, with the majority being European.

[161] *See*, *e.g.*, Robert D. Atkinson, *Don't Just Fix Safe Harbour, Fix the Data Protection Regulation*, EURACTIV (Dec. 18, 2015), http://www.euractiv.com/sections/digital/dont-just-fix-safe-harbour-fix-data-protection-regulation-320567 (containing a statement in which the president of a Washington-based think-tank urges reform of EU data protection law in order to facilitate data flows).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

and for reasons of US national security.[162] This has produced resentment in the EU about the extent of US lobbying on data protection,[163] and in the US about pressure from the EU to change its law.[164] An example of how political factors influence evaluations of the adequacy of protection in third countries can be seen in the fact that the Commission bases decisions on whether to begin a dialogue on adequacy on criteria such as "the extent of the EU's (actual or potential) commercial relations with a given third country" and "the overall political relationship with the third country in question."[165]

International political disagreements about data protection rights are to be expected because "rights to do not exist as such—'fact-like'—outside the structures of political deliberation."[166] Political disagreements are particularly likely with regard to a value such as privacy that is dependent on the cultural and social context in which it has arisen.[167] This is why transatlantic arguments about regulation of international data transfers tend to go around in circles, with each side justifying its own position based on its own underlying assumptions. The controversy about transatlantic data transfers is thus an example of the kind of *Justizkonflikt* that Schlosser wrote about in the 1980s regarding EU-US conflicts in civil procedural law, which he said was "rooted in political jurisprudence, and even to a large part in its sociological conditions."[168]

---

[162] *See*, *e.g.*, Stewart Baker, *Time to Get Serious About Europe's Sabotage of US Terror Intelligence Programs*, WASH. POST (Jan. 5, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/05/time-to-get-serious-about-europes-sabotage-of-us-terror-intelligence-programs/.

[163] *See*, *e.g.*, April Dembosky & James Fontanella-Khan, *US Tech Groups Criticized for EU Lobbying*, FIN. TIMES (Feb. 4, 2013), http://www.ft.com/intl/cms/s/0/e29a717e-6df0-11e2-983d-00144feab49a.html#axzz40hMUmieK; Francesco Guarascio, *US Lobbying Waters Down EU Data Protection Reform*, EURACTIV (Feb. 21, 2012), http://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/.

[164] *See*, *e.g.*, Katie Bo Williams, *Last-Minute Change to Privacy Bill Adds Tension to US-EU Talks*, THE HILL (Jan. 28, 2016), http://thehill.com/policy/cybersecurity/267401-last-minute-change-to-privacy-bill-adds-tension-to-us-eu-negotiations (quoting US Senator John Cornyn as stating with regard to adoption by the US of the Judicial Redress Act, which gives rights under the US Privacy Act to Europeans, when he stated that "U.S. companies should not have to endure regulatory threats in an attempt to change our policy or laws."). The Act was signed into law by President Obama on 24 February 2016. *See* Judicial Redress Act of 2015, *supra* note 17.

[165] *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World*, *supra* note 102, at 8.

[166] MARTTI KOSKENNIEMI, THE POLITICS OF INTERNATIONAL LAW 4421 (Kindle ed. 2011). *See also* J.H.H. Weiler, *Fundamental Rights and Fundamental Boundaries: On the Conflict of Standards and Values in the Protection of Human Rights in the European Legal Space*, *in* THE CONSTITUTION OF EUROPE: "DO THE NEW CLOTHES HAVE AN EMPEROR?" AND OTHER ESSAYS ON EUROPEAN INTEGRATION 106 (1999) (stating that "Human rights are almost invariably the expression of a compromise between competing social goods in the polity").

[167] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1219–1221 (2004).

[168] PETER SCHLOSSER, DER JUSTIZKONFLIKT ZWISCHEN DEN USA UND EUROPA 42 (Peter Schlosser trans., 1985).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

The problem is not that there is political disagreement about how to regulate international data transfers, but that the EU and the US often seem unwilling to consider positions that go beyond the underlying assumptions of their own systems. The Privacy Shield represents an attempt to break out of this cycle, but may well fall victim either to the unyielding standards of EU fundamental rights law, or unilateral action by the Trump administration, or both. The CJEU may also continue to chip away at the legal bases for transferring personal data, to the point that the few remaining options are no longer viable. In such a situation, there is the danger that EU law may retreat further into illusions, formality, and legal fictions in the application of data transfer regulation.

V. The Way Forward

Former European Data Protection Supervisor Peter Hustinx wrote in 2013 that the standards for international data transfers under the Directive are "based on a reasonable degree of pragmatism in order to allow interaction with other parts of the world."[169] The *Schrems* judgment shows that in fact, data transfer regulation in EU law is based not on reaching a reasonable accommodation between EU standards and those of other countries, but on a unilateral assertion of EU values. It is unrealistic to imagine that there can be a single, overarching legal "solution" to disputes about data transfer regulation unless the parties are willing to seek an accommodation that goes beyond the assertion of their own values. Protecting international data transfers is unlikely to be possible under bureaucratic, formalistic mechanisms that cannot provide real protection in practice.

Even if it cannot by itself resolve international disputes about data transfer regulation, the law may still serve as a "gentle civilizer of social systems,"[170] based on finding lines of compatibility and communication between different data protection systems. If one believes that EU data protection law cannot and should not shut itself off from other legal systems, and that Europeans want to be able to communicate internationally, then it is necessary to find a way to reach some kind of accommodation between EU data protection law and legal regimes in other regions. The new EU-US Privacy Shield will be an important test of the possibility of constructing stable bridges between different legal systems for privacy and data protection. Some of the elements of the Privacy Shield strengthen the perception of regulation of international data transfers as illusory, while others hold the potential of producing greater protection in practice. If it is not subject to a successful legal challenge,

[169] Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,* EUR. DATA PROT. SUPERVISOR 43 (Sept. 15, 2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf.

[170] Andreas Fischer-Lescano & Gunther Teubner, *Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law*, 25 MICH. J. INT'L L. 999, 1045 (2003).

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press

and assuming that it is shown to provide effective protection in practice, the Privacy Shield could serve as a model for protecting data flows from the EU to other regions as well.

Regulation of international data transfers in EU law must move beyond formalistic measures and legal fictions to implement actual protection in practice. It must also discard illusions, such as the idea that DPAs and national courts can perform large-scale assessments of the adequacy of non-EU data protection systems. Data protection law cannot by itself resolve issues relating to surveillance for national security or intelligence-gathering purposes, which will require further reform and transparency regarding intelligence-gathering practices. It will also be necessary for the CJEU or the EU legislator to clarify the application of data protection rights under the Charter to situations involving national security, in order to remove gaps in protection.

It is also essential that there be more enforcement of international data transfer regulation. At present, EU data protection law seeks to have its cake and eat it too by containing strict legal standards, but then rarely enforcing them in practice. If data transfer regulation is to regain its legitimacy, a choice will have to be made between taking enforcement measures when the law has been violated or changing the law. Widespread enforcement of data transfer regulation might produce difficult consequences, such as the disruption of international trade and cross-border communication. But being faced with such situations may be the crucible that forces the EU to make the difficult decisions necessary to adopt a system of data transfer regulation that is both adequate in theory and effective in practice.

The *Schrems* judgment forces us to face the contradictions of EU data transfer regulation squarely. It is no longer possible to ignore the legal and logical incoherence of data transfer regulation, or to pretend that an adequate level of data protection can be achieved on a global level by formalistic measures alone. Developing a more effective method of regulating data transfers also requires that other jurisdictions that aggressively assert their own regulatory visions, particularly the US, step back and see the debate between competing models of regulation from a broader perspective. This could provide common ground to overcome the illusions of the current data protection debate, and help bring the discussion back to reality.

https://doi.org/10.1017/S2071832200022197 Published online by Cambridge University Press