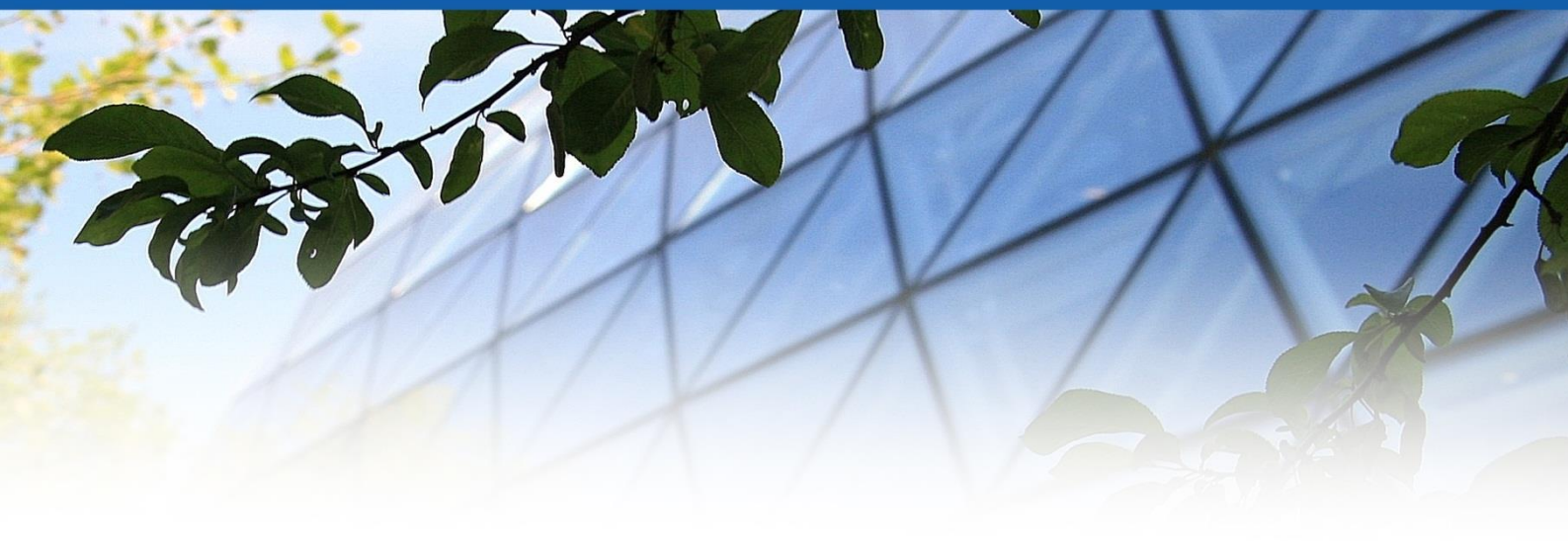
Legal Studies Research Paper Series

UNIVERSITY OF CAMBRIDGE
Faculty of Law



PAPER NO. 14/2016

MARCH 2016

Reality and Illusion in EU Data Transfer Regulation Post Schrems

Christopher Kuner

Further information about the University of Cambridge Faculty of Law Legal Studies Research Paper Series can be found at http://www.law.cam.ac.uk/ssrn/

Reality and illusion in EU data transfer regulation post *Schrems*

Christopher Kuner*

Version 1.0/March 2016

Abstract: In *Schrems v. Data Protection Commissioner*, the Court of Justice of the European Union invalidated the EU-US Safe Harbour arrangement allowing personal data to be transferred to the US. The judgment affirms the fundamental right to data protection, defines an adequate level of data protection for international data transfers under EU law, and extends data protection rights to third countries, all based on the EU Charter of Fundamental Rights. The judgment is a landmark in the Court's data protection case law, and illustrates the tension between the high level of legal protection for data transfers in EU law and the illusion of protection in practice. The judgment has undermined the logical consistency of the other legal bases for data transfer besides the Safe Harbour, and reactions to it have largely been based on formalism or data localization measures that are unlikely to provide real protection. *Schrems* also illustrates how many legal disagreements concerning data transfers are essentially political arguments in disguise. 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. It is crucial for data transfer regulation to go beyond formalistic measures and legal fictions, in order to move regulation of data transfers in EU law from illusion to reality.

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

I. 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, concerns about the misuse of personal data have put increased emphasis on the protection of international transfers of personal data. The most important body of data transfer regulation is that contained in Articles 25 and 26 of the EU Data Protection Directive[2] (the "Directive"), which restricts the transfer of personal data outside the EU unless an "adequate level of data protection" is provided based on EU legal standards.

* 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.

[1] Anton Chekhov, *Gooseberries*, in: *Selected Stories of Anton Chekov*, locations 5793-5794 (Kindle edition), Random House (2009), paraphrasing Alexander Pushkin.

[2] Directive 95/46/EC 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] OJ L281/31.

On 6 October 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*,[3] the CJEU invalidated the decision[4] 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[5] that preceded it provoked an intense public reaction, including front-page articles in major international newspapers;[6] a press conference by top officials of the European Commission;[7] reactions from US government officials;[8] a paper released by the Article 29 Working Party (the group of data protection authorities from the EU and its Member States);[9] concerned statements from US business organizations;[10] reactions from civil society groups;[11] opinions of academic experts;[12] legal memoranda from business groups;[13] and a newspaper interview by the President of the CJEU.[14]

[3] Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650.

[4] European 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] OJ L215/7. The alternative US spelling "Safe Harbor" will be used when it appears as such in original sources.

[5] Opinion of Advocate General Bot, Case 362/14, *Maximilian Schrems v. Data Protection Commissioner*, 23 September 2015, ECLI:EU:C:2015:650.

[6] See, e.g., Duncan Robinson, Richard Waters, and Murad Ahmed, "US tech companies overhaul operations after EU data ruling", Financial Times, October 6 2015, <http://www.ft.com/intl/cms/s/0/5d75e65a-6bf8-11e5-aca9-d87542bf8673.html#axzz3vvmkIE7x>; Mark Scott, "Data Transfer Pact between U.S. and Europe is Ruled Invalid", New York Times, 6 October 2015, <http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0>.

[7] European Commission, "First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems)", 6 October 2015, <http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm>.

[8] See speech by US FTC Commissioner Julie Brill, "Transatlantic Privacy after *Schrems*: Time for an Honest Conversation", 23 October 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", 28 September 2015, <http://useu.usmission.gov/st-09282015.html>.

[9] Article 29 Working Party, "The Court of Justice of the European Union invalidates the EU Commission Safe Harbour Decision", 6 October 2015, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf>.

[10] See, e.g., AmCham EU, "EU Court of Justice's decision in the Schrems case could disrupt transatlantic business, hurt the EU economy and jeopardise a Digital Single Market", 6 October 2015, <http://www.amchameu.eu/sites/default/files/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf>.

[11] EDRi, "EU and US NGOs propose privacy reforms post Schrems", 18 November 2015, <https://edri.org/eu-and-us-ngos-propose-privacy-reforms-post-schrems/>.

[12] Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms since 2013", 18 December 2015, <http://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf>.

[13] Sidley Austin LLP, "Essentially equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States", January 2016, <http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf>. This was prepared by the law firm Sidley Austin LLP on behalf of a number of US associations in the technology industry.

[14] See the linteview with CJEU President Koen Lenaerts in Valentina Popp, "ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust", The Wall Street Journal, 14 October 2015, <http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/tab/print/>.

In February 2016 agreement between the EU and the US was announced on a replacement for the Safe Harbour, called the "Privacy Shield",[15] regarding which details and supporting documentation were released on 29 February.[16] Further mechanisms to protect data transfers between the EU and the US are currently in the works, such as an agreement concerning data exchanges between law enforcement authorities,[17] and changes to US law to grant additional data protection rights to EU individuals.[18]

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

Viewed at a high level or "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 fruit produced by his gooseberry bushes are sweet, while in fact they are

---

[15] European Commission, "EU Commission and United States agree on a new framework for transatlantic data flows: EU-US Privacy Shield", 2 February 2016, <http://europa.eu/rapid/press-release_IP-16-216_en.htm>; US Department of Commerce, "EU-U.S. Privacy Shield", 2 February 2016, <https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield>.

[16] European Commission, "Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield", 29 February 2016, <http://europa.eu/rapid/press-release_IP-16-433_en.htm>, with links to the following documents that together comprise the Privacy Shield: Communication from the Commission to the European Parliament and the Council: Transatlantic Data Flows: Restoring Trust through strong Safeguards, COM(2016) 117 final, 29 February 2016; EU-US Privacy Shield: Frequently Asked Questions, 29 February 2016; Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the E.U.-U.S. Privacy Shield; Annex I, Letters from US Department of Commerce Secretary Penny Pritzker and US Under-Secretary for International Trade Stefan M. Selig, 23 February 2016; Annex II, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce; Annex III, Letter from US Secretary of State John Kerry, 22 February 2016; Annex IV, Letter from FTC Chairwoman Edith Ramirez, 23 February 2016; Annex V, Letter from US Secretary of Transportation Anthony R. Foxx, 19 February 2016; Annex VI, Letter from US General Counsel for the Office of the Director of National Intelligence Robert S. Litt, 22 February 2016; Annex VII, Letter from US Deputy Assistant Attorney General and Counselor for International Affairs for the Criminal Division Bruce C. Swartz, 19 February 2016.

[17] Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses (draft for initialling), 8 September 2015,<http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>. See also European Data Protection Supervisor, "Preliminary Opinion on the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offenses", 12 February 2016, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-02-12_EU-US_Umbrella_Agreement_EN.pdf>.

[18] H.R. 1428 – Judicial Redress Act of 2015, 114th Congress (2015-2016), signed by President Obama on 24 February 2016, <https://www.congress.gov/bill/114th-congress/house-bill/1428/all-actions?overview=closed>.

[19] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), Article 16, [2012] O.J. C 326/47.

[20] Charter of Fundamental Rights of the European Union, Article 8, [2010] O.J. C/83 389, 393

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 *Schrems* judgment affirms. This is a beautiful illusion, at least to European eyes, since 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 such as contractual clauses; and where DPAs police the Internet and quash attempts to misuse European data.

However, it remains an illusion, as can be seen by the measures that have been advocated in reaction to the *Schrems* judgment. Procedural mechanisms may satisfy formal requirements of data protection law, but 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 personal data on a broad scale, and raises other important legal issues.

The new EU-US Privacy Shield demonstrates both the reality and illusion of data transfer regulation. It represents a serious attempt to strengthen individual rights in line with the *Schrems* judgment, and is a much more detailed and weighty arrangement than the Safe Harbour. It also contains a number of novel mechanisms that could provide a basis for increasing trust in the protection given to international data transfers. However, it also demonstrates how EU data protection law tends to resolve questions concerning the regulation of international data transfers through verbose documentation and procedural mechanisms that are lengthy, untransparent, formalistic, and unintelligible to the average individual. It is also likely to be challenged before the CJEU.

In exploring the reality and illusion of protection for international data transfers, I will first summarize the judgment, before going on to examine its main holdings. In particular, I will analyse the Court's affirmation of the fundamental right to data protection and extension of its scope to third countries; its strengthening of the role of 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 is the EU Charter of Fundamental Rights, though some uncertainties remain because of the lack of EU competence over national security activities. I will also examine the concept of "essential equivalence" that the Court 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 also consider some legal issues presented by the Privacy Shield.

I will then move from the positivistic level to the meta level, and will discuss the implications of the judgment for other data transfer mechanisms provided for both in the Directive and in the EU General Data Protection Regulation (GDPR)[21] that will likely take effect in 2018. I will

[21] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January, 2012. At this time the final version of the GDPR has not yet been published in the EU Official Journal, but a version of 15 December 2015 agreed on between the Council and the European Parliament is available on the web site of the LIBE Committee of the Parliament at the following link: <http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884>.

examine the reactions to the judgment, and explain why they do not provide meaningful protection for data transfers. I will show how legal issues of data transfer regulation are intertwined with the underlying political positions of the parties involved, and will discuss the implications of the judgment for third countries. Finally, I will provide some suggestions for a way forward to move regulation of international data transfers from illusion to reality.

II. The judgment and its holdings

A. Background and facts

The facts of the judgment will be briefly summarized here. Further information is provided on the plaintiff's web site,[22] and in the judgment of the Irish High Court that resulted in the reference for a preliminary ruling being sent to the CJEU.[23]

The complainant, Mr. 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 number of principles based on EU data protection law with which Safe Harbour member companies had to commit to comply, and was overseen by the US Federal Trade Commission (FTC). In 2000 the Commission issued a formal decision under Article 25[24] of the Directive finding that transfers provide adequate protection under EU data protection law.

Following the Snowden revelations of 2013, which contained allegations of widespread surveillance of Internet data by the US intelligence agencies, Schrems then 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 Commission's determination of the Safe Harbour as providing adequate protection. Schrems argued that the DPC should use its statutory powers to find that no adequate protection existed under the Safe Harbour, 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 a judgment of 18 June 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

[22] See <http://europe-v-facebook.org/EN/en.html>.

[23] *Schrems v Data Protection Commissioner* [2014] IEHC 310; [2014] 2 ILRM 441; *Schrems v Data Protection Commissioner* (No.2) [2014] IEHC 351; [2014] 2 ILRM 506.

[24] Article 25(6) of the Directive (n 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."

> 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?"[25]

On 23 September 2015, Advocate General Bot delivered his opinion. He found that the two questions referred to the CJEU should be answered so that "the 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", and that the Safe Harbour decision of the Commission should be held invalid.[26]

B. Main holdings

On October 6, the Grand Chamber of the CJEU issued its judgment. The Court broadly agreed with the conclusions of Advocate General Bot 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 Commission decision, and that the decision underlying the Safe Harbour was invalid. The following were the main points that the Court 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 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 Court's case law interpreting the Charter (paras. 38-39). In considering the powers of the DPAs, the Court stressed the importance of their independence (paras. 40-43), and mentioned that their powers do not extend to data processing carried out in a third country (para. 44). However, 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 (para. 45) and the supervisory powers of the DPAs (para. 47). Since a 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 (para. 52).

However, a 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 (paras. 53-58). Such a claim is to be understood as essentially concerning "whether

[25] Reference for a preliminary ruling from High Court of Ireland (Ireland) made on 25 July 2014 – Maximillian Schrems v Data Protection Commissioner (Case C-362/14), <http://curia.europa.eu/juris/document/document.jsf?docid=157862&doclang=EN>.
[26] Opinion of Advocate General Bot (n 5), para. 237.

that decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals" (para. 59). Only the CJEU has the power to declare an EU act invalid, including a Commission adequacy decision (para. 61), and while national courts and the DPAs may consider the validity of an EU act, they may not themselves declare it invalid (para. 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" (para. 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 " (para. 64). Conversely, when the DPA finds such claim to be well-founded, it must "be able to engage in legal proceedings", and the national legislature must "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" (para. 65).

The Court then considered the validity of the Safe Haber 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 (para. 67). The Court went on 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", while not requiring that the level be identical to that under EU law (para. 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" (para. 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 (para. 74).

When assessing the level of protection in a third country, this requires the Commission to "take account of all the circumstances surrounding a transfer of personal data to a third country" (para. 75), to check periodically whether the adequacy assessment is still justified (para. 76), and to take account of circumstances that have arisen after adoption of the decision (para. 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" (para. 78).

The Court then dealt with the validity of the adequacy decision regarding the Safe Harbour. 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 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" (para. 81). It noted that public authorities in the US are not required to comply with the Safe Harbour principles (para. 82), and that the Safe Harbour decision of the Commission does not contain sufficient findings explaining how the US ensures an adequate level of protection (para. 83).

The CJEU then noted that under the Safe Harbour decision, the applicability of the principles may be limited to meet, for example, national security, public interest, or law enforcement requirements (para. 84), and that 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'" (para. 85). It found that these provisions in effect give US law primacy over EU fundamental rights in situations where they conflict (paras. 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" (para. 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 (para. 88).

The Court then referred to previous statements by the Commission that "the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security" (para. 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 (para. 91), and that derogations and limitations in relation to data protection should apply only when strictly necessary (para. 92), and found that US law does not meet these standards (para. 93-95).

Of particular importance is the Court's statement that "legislation is not limited to what is strictly necessary where it authorises, on a generalised 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" (para. 93). The Court found that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the *essence* of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter" (para. 94), and 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" (para. 95) (emphasis added in both cases).

The Court went on to note that the Commission did not state in its Safe Harbour decision that the US ensures an adequate level of protection (para. 97), and that the decision was accordingly invalid, without there being any need for it to examine the substance of the Safe Harbour principles (para. 98). Throughout this section of the judgment, the CJEU makes extensive reference to its earlier ruling in *Digital Rights Ireland*,[27] in which the Court strongly affirmed data protection rights in the digital context. The Court also found that Article 3 of the Safe Harbour decision contained impermissible limitations on the powers of the data protection authorities (paras. 99-104).

III. Main themes of the judgment

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

A. Affirming the right to data protection

The judgment strongly affirms data protection as a fundamental right under EU law. The Court makes repeated reference to fundamental rights under the Charter, and to previous data protection judgments such as *Digital Rights Ireland* and *Google Spain*.[28] This emphasis on fundamental rights is further seen in statements such as that the Commission's discretion in pronouncing on the adequacy of protection in third countries should be "strict" (para. 78).

Particularly significant is the fact that the Court found that generalized access to data by public authorities (i.e., law enforcement authorities) compromises the "essence" of the right to private life under Article 7 of the Charter, since this means that no proportionality or balancing analysis involving other rights and freedoms under the Charter is required with regard to such violation.[29] At the same time, it is unclear how the Court could find a violation of the essence of right to privacy under Article 7 but not one of the essence of the right to the protection of personal data under Article 8. The rights to data protection and privacy are closely linked, and surveillance of data by intelligence services self-evidently involves the processing of personal data. In its *Digital Rights Ireland* judgment in which the Court invalidated the EU Data Retention Directive,[30] it found that the essence of the right to data protection was not violated since the Directive required respect for "certain principles of data protection and data security",[31] an argument that seems questionable since data security, while certainly important, is not one of the central elements of data protection. The Court's interpretation of the essence of the rights to privacy and data protection in *Schrems*

[27] *Digital Rights Ireland and Seitlinger*, Joined Cases C-293/12 and C-594/12, 8 April 2014, ECLI:EU:C:2014:238.
[28] *Google Spain v. AEPD and Mario Costeja Gonzalez*, Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.
[29] See Martin Scheinin, "The Essence of Privacy, and Varying Degrees of Intrusion", Verfassungsblog, 7 October 2015, <http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion/>.
[30] Directive (EC) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (EC) 2002/58, [2006] OJ L105/54.
[31] *Digital Rights Ireland and Seitlinger* (n 27), para. 40. For a criticism of the Court's analysis in *Digital Rights Ireland*, see Orla Lynskey, *The Foundations of EU Data Protection Law* 270-272 (Oxford University Press 2015).

may thus reflect its longstanding confusion about the distinction between these two rights.[32]

B. Extending data protection rights to third countries

The Court indicated that while it was not directly applying EU law to third countries (para. 44), EU law applied to data transfers since "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".[33] While it may be logical to distinguish between the direct application of EU law in a third country and the transfer of EU-based data to such country, in the end this is a distinction without a difference, since, as the *Schrems* judgment makes clear, such transfer is possible only when the third country provides protections that are "essentially equivalent" to those under EU law. The *Schrems* case thus illustrates that any distinction between extraterritorial and territorial jurisdiction has become meaningless in the context of regulation of international data transfers .[34]

The Court's only previous case dealing specifically with regulation of international data transfers was its *Lindqvist* judgment of 2003,[35] 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 high level of data protection required by Charter.[36] It thus seems that the Court believes that a high level of data protection is required under the Charter for data transfers to third countries, and that, if it were faced today with a case involving facts similar to those in *Lindqvist*, it would be more hesitant to find that Article 25 does not apply to placing personal data on an Internet site, since this will result in access to EU data in countries where the level of data protection may not be adequate.

By determining the standard that third countries must meet to be declared "adequate" in the eyes of the EU, the CJEU has effectively set the global data protection bar at a high level. Many third countries will revise their data protection law and practice in an attempt to meet this standard, so that the conclusions of the Court will reverberate around the world.

Bradford has referred to the so-called "Brussels effect", in which the EU is engaged in unilateral regulation of global markets,[37] which can be seen in the influence that EU data

[32] See regarding the connection between the rights to data protection and privacy in the Court's jurisprudece Lynskey (n 31), at 89-130 (Oxford University Press 2015); Juliane Kokott and Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", 3 International Data Privacy Law 222 (2013); Hielke Hijmans and Alfonso Scirocco, "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?", 46 Common Market Law Review 1485 (2009).

[33] *Schrems* (n 3), para. 45.

[34] For criticism of the distinction between territorial and extraterritorial jurisdiction in the context of regulation of international data transfers, see Christopher Kuner, "Extraterritoriality and regulation of international data transfers in EU data protection law", 5 International Data Privacy Law 235 (2015).

[35] *Bodil Lindqvist*, Case C-101/01 [2003] ECR I-12971.

[36] *Schrems* (n 3), para. 73.

[37] See Anu Bradford, "The Brussels Effect", 107 Northwestern University Law Review 1 (2013). For a critical view of the this argument, see Joanne Scott, "The new EU 'extraterritoriality'", 51 Common Market Law Review

protection law has had on the development of data protection legislation in many third countries.[38] The *Schrems* judgment can be seen as an indirect example of the Brussels effect, since 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.[39]

The irony is that the judgment results in withdrawal of regulatory recognition from a mechanism (i.e., the Safe Harbour) that did influence such standards. Despite the criticisms that caused the CJEU to invalidate the Safe Harbour, research into compliance with privacy "on the ground" has found that EU law in general, and the Safe Harbour in particular, have played a major role in shaping how companies in the US process personal data.[40] For example, regulators in the US have explained that the invalidation of the Safe Harbour may weaken the protection of personal data transferred from the EU to the US, first by making the protection given to it less transparent, and second by limiting the ability of the US Federal Trade Commission to take action against companies in the US for misrepresenting their compliance with EU data protection standards.[41] Time will tell if new Privacy Shield, which includes strengthened versions of the standards contained in the Safe Harbour and also provides for enforcement by the FTC, will lead to further influence of EU data protection concepts on US practices.

C. Increasing both the role of DPAs and their burdens

By confirming that DPAs may not be precluded from examining the level of data protection in a third country set out in Commission adequacy decisions, the Court has substantially strengthened their role at the expense of that of the Commission. At the same time, the judgment practically invites individuals to bring claims regarding adequacy to DPAs, who are then required to use "all due diligence" to examine them.[42] The DPAs are notoriously short on personnel and resources,[43] and evaluating the level of data protection in third countries can be a complicated exercise, so this new role will put substantial pressure on them.

1343 (2014); Joanne Scott, "Extraterritoriality and Territorial Extension in EU Law", 62 American Journal of Comparative Law 87 (2014).

[38] See Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014), at locations 6215-6216 (Kindle edition); Paul De Hert and Vagelis Papakonstantinou, "Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", I/S: A Journal of Law and Policy for the Information Society, vol. 9, no. 2, 2013, 271-324, at 287-288; Graham Greenleaf, "The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108", 2 International Data Privacy Law 68 (2012). See regarding the influence of EU data transfer regulation in other legal systems Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013).

[39] See interview with CJEU President Koen Lenaerts (n 14), in which he states "If 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?"

[40] Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Ground* (MIT Press 2015), at 65, 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".

[41] Brill (n 8), at 6.

[42] *Schrems* (n 3), para. 78.

[43] 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>.

Article 25 was intended to lead to a harmonized procedure for Commission adequacy decisions,[44] but under the judgment, DPAs may investigate complaints from individuals concerning adequacy decisions, though they may not themselves declare a decision illegal. In such investigations, the DPAs may make use of the powers granted to them by national law under Article 28 of the Directive, which the Court 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".[45] If a DPA finds such a claim to be well-founded, then it must be able to engage in legal proceedings, which presumably means that it must be able to make use of the powers granted to it by legislation and to call on the national courts to help enforce them if necessary. The national legislator must enact legislation allowing the DPAs to provide for legal remedies, and if a national court is involved in a case in which it has doubts about the validity of a Commission adequacy decision, the court must make a reference for a preliminary ruling to the CJEU to examine the decision's validity.

The judgment may result in a patchwork of different views among the DPAs and Member State courts on the level of protection in third countries, which could lead to uneven protection for individuals throughout the EU.[46] Such fragmentation effectively defeats the purpose of adequacy decisions by subjecting them to differing national interpretations, and by miring them in regulatory procedures and litigation as to their validity. Presumably the fact that the CJEU is the final arbiter of what constitute adequate protection will reduce the fragmentation, and with the GDPR being a highly-detailed EU regulation, under it the DPAs will have to take a harmonized view of what constitutes adequate protection.[47] The so-called consistency and cooperation mechanisms of the GDPR, 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), should also hopefully lead to a more harmonised view of adequacy in third countries. However, it can take years for a case to reach the CJEU, and under the GDPR each individual DPA will have the power to suspend data transfers to third countries.[48] Thus, it seems there is the potential for a difference of views regarding adequate protection in third countries, with resultant legal uncertainty.

D. Defining an adequate level of data protection

[44] See Spiros Simitis and Ulrich Dammann, *EG-Datenschutzrichtlinie* (Nomos 1997), at 275.
[45] *Schrems* (n 3), para. 43.
[46] See European Commission, "Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century", COM(2012) 9 final, 25 January 2012, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en>, at 7, stating that the current fragmentation of data protection law in the EU has led to "uneven protection for individuals",
[47] See Stefanio Melloni v Ministerio Fiscal, Case C-399/11, 26 February 2013, ECLI:EU:C:2013:107, in which the CJEU found 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. But see Peter Blume and Christian Wiese Svanberg, "The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus", in Catherine Barnard et al. (eds.), 15 *Cambridge Yearbook of European Legal Studies* 27 (Hart Publishing, 2012-2013), arguing that there will be many exceptions to harmonization under the GDPR.
[48] Article 53(1b)(h) of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21).

The most controversial issue dealt with in the judgment is the Court'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 Court 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 risks of gaps in the level of data protection, which should be addressed by the EU legislator and the Court.

1. EU standards and third country standards

The "elephant in the room" in the debate about the definition of an adequate level of protection is the criticism in the judgment of US intelligence surveillance practices. The *Schrems* judgment does not make any explicit statements concerning the adequacy of the US legal system as a whole, US legal rules concerning intelligence surveillance, or the details of the Safe Harbour.[49] However, 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, as can be seen, for example, in its Court's mention of studies by the Commission finding 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.[50]

Some argue that it is hypocritical for EU policymakers and the CJEU to concern themselves in such detail with the standards of data protection for intelligence surveillance outside the EU, when the standards that apply in the EU seem lacking in many respects.[51] Under Article 4(2) of the Treaty on European Union (TEU),[52] national security remains the sole responsibility of the EU Member States, and activities concerning national security are outside the scope of the EU Data Protection Directive and the GDPR.[53] In addition, it seems that there is widespread sharing of information between the US and other intelligence services, such as under the "Five Eyes"[54] intelligence-sharing network which includes the UK (the other members are Australia, Canada, New Zealand, and the US).

---

[49] See *Schrems* (n 3), paras. 88 and 98. See also inteview with CJEU President Koen Lenaerts (n 14), in which he states "We 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".

[50] See *Schrems* (n 3), para. 90.

[51] See, e.g., Opinion of Geoffrey Robertson QC for Facebook, 14 January 2016, <http://blogs.ft.com/brusselsblog/files/2016/01/Geoffrey-Robertson-QC.docx>); Sidley Austin LLP, "Essentially equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States" (n 13). See regarding oversite of intelligence surveillance in the Member States, European Union for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", November 2015, <http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf>; Stefan Heumann and Ben Scott, "Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany", September 2013, <http://www.stiftung-nv.de/publikation/law-and-policy-internet-surveillance-programs-united-states-great-britain-and-germany>.

[52] Consolidated Version of the Treaty on European Union, [2012] O.J. C 326/13.

[53] EU Data Protection Directive (n 2), Article 3(2)) and Recital 14 of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21), exempting matters of national security from the scope of the Directive and the GDPR.

[54] See regarding the Five Eyes alliance Glenn Greenwald, *No Place to Hide* (Penguin 2014), at locations 1581, 1854-1900 (Kindle edition).

However, it is pointless for the EU and the US to engage in arguments about which side's system of data protection is better, since this is irrelevant for the standard of protection articulated by the Court. A violation of fundamental rights by a third country cannot be excused because EU standards may themselves be lacking, and arguments along these lines are examples of a logical fallacy known as "tu quoque" ("you too"). While such objections may be understandable, there is no parallel in EU law to the common law doctrine of "unclean hands" which may underlie the arguments along these lines by US commentators.[55]

2. The Charter as the standard, with questions regarding national security

From a legal point of view, the main issue is what standard should be used to measure essential equivalence as the Court has defined it. Despite uncertainties caused by the allocation of competence over national security to Member States, the correct measure is provided by the EU Charter of Fundamental Rights.

The Court states several times in the *Schrems* judgment that the fundamental right to data protection is to be measured against the Charter,[56] and makes frequent references both to the Charter and to previous judgments applying it, in particular *Digital Rights Ireland*. It also points out that the standard for an adequate level of protection is high,[57] and that the Commission's review of requirements deriving from Article 25 of the Directive should be read strictly in light of the Charter.[58] The Court's assessment of fundamental rights also seems to be based solely on the Charter in the vast majority of cases.[59] Thus, there seems little doubt that the Charter should be the measure of protection for international data transfers from the EU.

While provisions such as Article 4(2) TEU place the competence for national security with the Member States, the allocation of legislative competences in EU law is not the same as the scope of application of the Charter.[60] The Charter applies to the Member States when they implement EU law,[61] and thus applies to situations covered by the Directive (for example, when EU companies acting as data controllers transfer data to EU or third country intelligence services).[62] There are many data protection situations involving national security where the Charter does apply, such as to questions about whether national legislation

---

[55] See regarding the unclean hands doctrine and tu quoque arguments, Kevin W. Saunders, "Informal Fallacies in Legal Argumentation", 44 South Carolina Law Review 343, 373-374 (1992).

[56] See, e.g., *Schrems* (n 3), paras. 38 ("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") and 67 ("it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter").

[57] Ibid, paras. 39, 72, and 73.

[58] Ibid., para. 78.

[59] Clara Rauchegger, "The Interplay Between the Charter and National Constitutions after *Åkerberg Fransson* and *Melloni*", in: Sybe de Vries, Ulf Bernitz and Stephen Weatherill (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument* 93, 122 (Hart 2015).

[60] Rauchegger (n 59), at 97.

[61] Charter, Article 51(1). See Rauchegger (n 59), at 97.

[62] European Union for Fundamental Rights, "Surveillance by intelligence services" (n 51), at 11.

restricting data protection rights for reasons of national security is valid under Article 13(1)(a) of the Directive,[63] and to investigations regarding such restrictions by DPAs under Article 28(4) of the Directive.[64]

Nor does the fact that Article 4 place 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 fundamental rights of EU individuals. Neither the TEU nor the Directive explicitly or implicitly remove the activities of third countries from scrutiny under EU law. The territorial scope of the Charter is the same as that of EU law,[65] and to the extent that EU law can apply to the activities of third country intelligence agencies, the Charter should as well.

At the same time, the allocation of responsibility for national security to 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, as the *Schrems* judgment shows, but on the other hand, national security activities are wholly carried out by the Member State. There is thus a divergence between the level at which applicable fundamental rights law is enacted (i.e., at the EU level) and that at which national security activities are actually carried out (i.e., by the Member States). In many or most 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 of the Charter. However, when EU law does not apply, such situations are governed solely by Member State constitutional law.[66] This could produce a gap in protection if Member State law produces a lower level of protection than the Charter.

It will also not always be possible to distinguish situations where personal data are processed for national security purposes. In most routine situations personal data are transferred for purposes that have nothing to do with national security (e.g., for commercial or personal reasons), but there are many situations where the purposes of transfer may be mixed so that it is impossible to distinguish them, i.e., when data are collected or transferred for commercial purposes but then accessed by national intelligence agencies after the fact.[67]

---

[63] Article 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…" Article 21 of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21) also allows restrictions to be put on data protection rights for national security reasons under strict conditions.

[64] Article 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."

[65] See Violeta Moreno-Lax and Cathryn Costello, "The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model", in: Steve Peers, Tamara Harvey, Jeff Kenner and Angela Ward (eds.), *The EU Charter of Fundamental Rights, A Commentary* (Hart Publishing 2014), at 1657-1683.

[66] See Bruno de Witte, "Article 53—Level of Protection", in: Peers et al. (n 65), at para. 53.12 (Kindle edition), stating "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".

[67] See in this regard Fred H. Cate, James X. Dempsey, and Ira S. Rubenstein, "Systematic government access to private-sector data", 2 International Data Privacy Law 195 (2012).

It seems likely that the Court would take a restrictive view of claims that the Charter should not apply to data protection issues involving national security. Under Article 53 of the Charter nothing in it can be interpreted as adversely affecting human rights, and the constitutional autonomy of EU law, which the Court has taken pains to emphasize,[68] would not tolerate a lowering of the level of fundamental rights under the Charter based on the positions of some Member States or a margin of discretion or margin of appreciation based on the European Convention of Human Rights.[69] The official Explanations to the Charter prepared under the 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.[70] The Charter is intended to prevent a "race to the bottom" in fundamental rights standards,[71] such as could occur if low standards in certain Member States were taken at 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 in order to remove their activities from scrutiny under EU fundamental rights law.[72]

However, the unclear delineation and definition of "national security" can produce confusion about the standards that should apply to Member State activities.[73] There is an urgent need for limitation or clarification of the meaning of "national security" in the context of data protection rights. The Charter requires that the meaning and scope of rights under it shall be "the same" as under the European Convention on Human Rights,[74] which is not limited by any derogation for national security, and clarification could come via challenges to Member State intelligence surveillance practices brought before the European Court of Human Rights.[75] It is to be hoped that a case involving the allocation of national security to the Member States will reach the CJEU as well, in order to clarify the conditions under which the Charter applies to data protection issues that are affected by national security activities.

---

[68] See Opinion 2/13 of the Court, 18 December 2014, CLI:EU:C:2014:2454.

[69] See Koen Lenaerts and Jose Antonio Gutierrez-Fons, "The Place of the Charter in the EU Constitutional Edifice", in: Peers et al. (n 65), at para. 55.60 (Kindle edition), stating "if the ECtHR ever decides 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 intepreting the provisions of the Charter in a regressive fashion."

[70] "Explanations Relating to the Charter of Fundamental Rights", [2007] OJ C303/17, at C303/34.

[71] Rauchegger (n 59), at 125.

[72] See *ZZ v. Secretary of State for the Home Department*, Case C-300/11, 4 June 2013, ECLI:EU:C:2013:363, para. 38, where the Court held 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 *P.I. v. Oberbürgermeisterin der Stadt Remscheid*, Case C-348/09, 22 May 2012, EU:C:2012:300, stating at para. 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 a Constitutional Guardian of Internet Privacy and Data Protection: the story of Article 16 TFEU* 157-162 (PhD thesis, University of Amsterdam and Vrije Universiteit Brussel, 2016).

[73] See European Union for Fundamental Rights, "Surveillance by intelligence services" (n 51), at 11.

[74] Charter, Article 52(3).

[75] *Big Brother Watch and Others v. The United Kingdom*, Case No. 58170/13 (pending).

3. The meaning of "essentially equivalent"

In the *Schrems* judgment, the Court 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.[76] It did so despite the fact that when the Directive was adopted, the EU legislator specifically preferred the term "adequate protection" over "equivalent protection".[77] The Court gave a number of points of orientation to interpret the concept of essential equivalence, including the following (with parenthetical citations to the judgment):

--There must be a high level of fundamental rights protection under the Charter and the Court's case law interpreting the Charter (paras. 38-39, 73), which should be judged strictly (para. 78).
--The third country in question must have a means for ensuring a high level of protection that is effective in practice (para. 74), in light of all the circumstances surrounding a transfer of personal data to a third country (para. 75). This must include periodic checks as to whether the adequacy assessment is still justified (para. 76) and take into account all circumstances that have arisen after adoption of the decision (para. 77).
--Adequate protection must take into account the country's domestic law or international commitments (para. 71).
--Any system of self-certification must be reliable 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 (para. 81).
--An adequacy decision must include a detailed explanation of how a country ensures an adequate level of protection (para. 83).
--There must not be limitations based on national security, public interest, or law enforcement requirements that give third country law primacy over EU law (paras. 85-87).
--Limitations must be placed on the power of public authorities (such as law enforcement authorities) to interfere with fundamental rights (para. 88). In particular, any such access must be strictly necessary and proportionate to the protection of values such as national security (para. 90), there must be clear and precise rules regarding the scope of application of a measure, and for effective protection against the risk of abuse of data (para. 91), and derogations and limitations in relation to data protection should apply only when strictly necessary (para. 92).
--Third country legislation must not authorize, on a generalised 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 (para. 93).

This is a high standard that results from the Court's strict interpretation of the Charter, and its previous judgments such as *Google Spain* and *Digital Rights Ireland*. The Court further emphasized the primacy that must be given to EU fundamental rights over conflicting third

[76] *Schrems* (n 3), para. 73.
[77] Simitis and Dammann (n 44), at 273.

country norms. The Article 29 Working Party has condensed these factors into a rather superficial four-part test for determining adequacy:[78]

> "A. Processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;
> B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual;
> C. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;
> D. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body."

The term "essentially equivalent" seems to imply a comparison between third country data protection standards and EU standards, an enterprise that is fraught with difficulty. Data protection and privacy are "context-bound and linked to culture",[79] making them difficult areas for comparative analysis. There are numerous theories used to compare different systems and concepts of constitutional and public law,[80] and selecting and refining the correct methodological approach in order to evaluate foreign legal systems of data protection is a lengthy and highly complex process. The European Commission has internal guidelines for conducting such studies, which have never been made public, but it is known that they typically can take several years and involve extensive participation by outside academic experts in foreign law. Comparison of legal systems is not a mechanical exercise, and particularly in an area like data protection requires going beyond analysis of legal texts to consider non-legal and social factors,[81] including ones such as constitutional protection, treaty protection, human rights institutions, civil law protection, criminal law and administrative law, and self regulation.[82]

The *Schrems* judgment foresees DPAs being able to question Commission adequacy decisions, and individuals being able to challenge them before national courts. One can be sceptical about how a DPA, with its limited resources, or a national court, with its focus on national or EU law, can conduct a sufficient examination of foreign law and a comparison with EU data protection law, particularly with regard to third countries like the US that have

---

[78] "Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment", 3 February 2016, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf>.
[79] Manuel José Cepeda Espinosa, "Privacy", in: Michel Rosenfeld and András Sajó, *The Oxford Handbook of Comparative Constitutional Law* (Oxford University Press 2012), at 967 (Kindle edition). This is true even between the different EU Member States. See M Cartabia, "Europe and Rights: Taking Dialogue Seriously", 5 European Constitutional Law Review 5, 20 (2009).
[80] Vicki C. Jackson, "Comparative Constitutional Law: Methodologies", in Rosenfeld and Sajó (n 79), at 54 (Kindle edition), mentioning classificatory, historical, normative, functional, and contextual approaches.
[81] See, e.g., Günter Frankenberg, "Critical Comparisons: Re-thinking Comparative Law", 26 Harvard International Law Journal 411 (1985).
[82] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014), at 53.

not enacted a horizontal system of data protection similar to EU law. Since 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,[83] there is a risk that the decision of whether essential equivalence exists could be made on the basis of an insufficient evaluation of foreign law or on political pressures. Since intervention in references to the CJEU for a preliminary ruling is not possible,[84] there is no chance for third parties (such as foreign governments or academic experts) to intervene in such proceedings in order to provide further clarification on data protection standards in third countries.

There is thus a risk that determinations about essential equivalency may become another example of illusory protection. This makes it important in the future for third countries to monitor proceedings in national courts regarding the validity of adequacy decisions concerning them and attempt to intervene in such proceedings at the national level when possible, since all parties to the main proceedings at the national level may then participate in the procedure before the CJEU.[85] The CJEU could also consider ordering measures of inquiry (such as expert reports) pursuant to its Rules of Procedure,[86] which is permitted in a preliminary ruling on the validity of an EU act (for example, the European Data Protection Supervisor (EDPS) was invited to submit observations to the Court in the *Schrems* case based on this provision).

Perhaps too much attention has been given to the term "essentially equivalent" as used by the Court. The Court's intention seems to have been to emphasize that the level of protection that third countries must meet 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, parsing the linguistic meaning of the terms "essentially" and "equivalent" is less likely to lead to a meaningful understanding of the standard the Court requires than does examining the data protection standards required by the Charter and its interpretation by the CJEU in cases like *Digital Rights Ireland* and *Schrems*.

4. Coda: The EU-US Privacy Shield

On 2 February 2016, the EU and the US announced that they had agreed on the Privacy Shield as a replacement for the Safe Harbour,[87] and a draft adequacy decision, together with supporting documents, was published on 29 February. The documentation is voluminous (130 pages) and cannot be discussed in detail here, but the European Commission summarizes the Privacy Shield as comprising "strong obligations on companies and robust

[83] See Koen Lenaerts, Ignace Maselis, and Kathleen Gutman, *EU Procedural Law* (Oxford University Press 2014), at location 15562 (Kindle edition), 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".
[84] Ibid., at location 23573 (Kindle edition).
[85] Ibid.
[86] Ibid., at locations 19002-19015 (Kindle edition), noting that in such cases "it would be perfectly possible for measures of inquiry to be ordered pursuant to Art. 64(2) of the ECJ Rules of Procedure". Article 64(2) foresees such measures as "the commissioning of an expert's report".
[87] See n 15.

enforcement", "clear safeguards and transparency obligations on U.S. government access", "effective protection of EU citizens' rights with several redress possibilities", and an "annual joint review mechanism".[88]

The Privacy Shield is much more detailed than the Safe Harbour, and includes stronger protections in certain areas.[89] In contrast with the Safe Harbour, it 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. Reflecting two years of negotiation,[90] the Privacy Shield represents a bold attempt to put transatlantic data transfers back on a solid legal footing.

At the same time, there are a number of questions that can be raised about it. Presumably because of political pressures to have it enacted quickly, there will apparently not be any assessment of the Privacy Shield by independent academic experts before the Commission proposes it for approval. The documentation that comprises the Privacy Shield is lengthy and structured in a haphazard way, making it difficult for individuals and small companies to interpret it. Many of the supporting letters from US officials are written in US legalese and will be difficult for many people in the EU to understand.

The way the Privacy Shield was drafted and presented demonstrates how regulation of international data transfers is dealt with in a predominantly untransparent and bureaucratic way. The *Schrems* judgment presented the ideal opportunity to reflect on the effectiveness and coherence of EU regulation of data transfers, and to hold an open discussion with experts and the public as to how it should be improved. Instead, the EU and the US intensified their secret negotiations on a successor to the Safe Harbour, and then revealed the final package while stressing the need to adopt it as quickly as possible.[91]

Several further steps are necessary before the Privacy Shield comes into force (i.e., approval by the Article 29 Working Party and the EU Member States), so it could be some time before the first data transfers are carried out under it. The Privacy Shield will also no doubt be the subject of legal challenges before the DPAs and, ultimately, before the CJEU, and will remain under a cloud until they are resolved. An as instrument of EU law, implementation of the Privacy Shield will have to meet strict standards of proportionality, legality, legitimate interest, and compliance with fundamental rights under the Charter.[92]

The following are a few major legal questions that will have to be answered (most likely by

---

[88] European Commission, "Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield" (n 16).

[89] For example, with regard to onward transfers of personal data transferred to the US under the Shield. See U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), para. III, at 5-6.

[90] See Annex I, Letters from US Department of Commerce Secretary Penny Pritzker and US Under-Secretary for International Trade Stefan M. Selig (n 16), at 1, stating that the Privacy Shield is "the product of two years of productive discussions".

[91] See , e.g., Zoya Sheftalovich, "5 takeaways from the privacy shield", politico.com, 29 February 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".

[92] Lenaerts and Gutierrez-Fons (n 69), at location 50666 (Kindle edition).

the CJEU) if the Privacy Shield is not to suffer the same fate as the Safe Harbour:

--The CJEU in *Schrems* found that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter" (para. 94). Thus, under the Charter, such access is per se unlawful, without the need for a balancing test. The Privacy Shield presents a confusing picture with regard to its coverage of mass surveillance or the bulk collection of data by US intelligence or national security agencies. On the one hand, in the documentation the European Commission states that "The US assures there is no indiscriminate or mass surveillance on the personal data transferred to the US under the new arrangement",[93] and the US notes that under US law, bulk collection of data or mass surveillance is "prohibited".[94] On the other hand, the US also states in the documentation that "signals intelligence collected in bulk can only be used for six specific purposes",[95] and that "any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet",[96] suggesting that bulk collection does occur. The European Commission itself seems lukewarm about the degree of protection that the Privacy Shield provides with regard to US national intelligence activities: while the Commission's draft adequacy decision states that the Privacy Shield principles issued by the US Department of Commerce as a whole ensure a level of protection of personal data that is "essentially equivalent" to that under EU law,[97] it refers to the protection granted by the Privacy Shield against interference by US law enforcement and other public authorities merely as "effective".[98]

--In *Schrems* the Court criticized the Safe Harbour for giving US law primacy over EU fundamental rights.[99] However, the obligations contained in the Privacy Shield are to be interpreted under US law,[100] and it provides broad derogations from its principles in situations when this is necessary "to meet national security, public interest or law enforcement requirements",[101] or in situations where US law may create conflicting

[93] EU-US Privacy Shield: Frequently Asked Questions (n 16), at 2.
[94] Annex VI, Letter from US General Counsel for the Office of the Director of National Intelligence Robert S. Litt (n 16), at 13, stating that the USA Freedom Act "prohibits bulk collection of any records, including of both U.S. and non-U.S. persons…"
[95] Ibid., at 4.
[96] Ibid.
[97] Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the E.U.-U.S. Privacy Shield (n 16), at 29 (Recital 113).
[98] Ibid at 28-29 (Recitals 111 and 116).
[99] See *Schrems* (n 3), para. 86, stating "Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them."
[100] See U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), para. I(7), at 2. The emphasis on the primacy of US law is further emphasized by the fact that for arbitration proceedings under the Privacy Shield, it is stated that "arbitrators…must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law" (Annex II, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), at 33).
[101] Commission Implementing Decision (n 16), para. 52; U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), at 2.

obligations.[102] It also gives priority to freedom of expression under the First Amendment to the US Constitution over conflicting obligations, which may be interpreted to include the "right to be forgotten" that the CJEU recognized in *Google Spain*.[103] It could be difficult for the Court to tolerate giving US law priority over EU fundamental rights, particularly in light of its other judgments that emphasize the status of EU law as an autonomous legal system.[104]

--Many of the guarantees in the Privacy Shield are based on assurances given in letters and other supporting documents from US officials, some of whom are political appointees. It seems that such assurances could be changed or revoked at will, and that many of these officials may change jobs or leave the government when the Obama Administration leaves office. While these documents are all to be published in the US Federal Register,[105] such publication merely "provides the public official notice of a document's existence, specifies the legal authority of the agency to issue the document, and gives the document evidentiary status."[106] The Charter requires that any limitation of fundamental rights must be "provided by law",[107] which the Court has generally interpreted to mean a legal measure of the EU or of a Member State,[108] and which it requires to meet certain qualitative standards such as being clear, accessible, and foreseeable.[109] The question is whether the underlying assurances granted by US officials that constitute a key part of the guarantees to be included in the proposed Commission decision would fulfil the requirement of "provided by law" under the Charter.

--A new "Privacy Shield Ombudsman" function is to be created within the US Department of State, which is to be independent from the intelligence agencies and is supposed to follow up complaints and inquiries from individuals regarding intelligence surveillance. Questions can be raised as to whether the Ombudsman, who is a high official in the US Department of State,[110] would fulfil the criteria set by the CJEU for an independent regulator. In particular, the Court has emphasized that data protection regulators must be independent from external influence (including that from inside the government), not just independent vis-à-vis the entity being regulated.[111] The European Ombudsman has already questioned whether this new function would actually be independent under internationally-recognized

---

[102] U.S.-EU Privacy Shield Framework Principles Issued by the U.S. Department of Commerce (n 16), at 2, stating " Adherence to these Principles may be limited: … (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization".

[103] Ibid., para. III(2), at 8.

[104] See Opinion 2/13 of the Court, 18 December 2014, CLI:EU:C:2014:2454; Joined Cases C-402 & 415/05P, Kadi & Al Barakaat Int'l Found. v. Council & Commission, [2008] ECR 1-6351.

[105] "EU-US Privacy Shield: Frequently Asked Questions" (n 16), at 2.

[106] Amy Bunk, "Federal Register 101", <https://www.federalregister.gov/uploads/2011/01/fr_101.pdf>.

[107] Charter, Article 52(1).

[108] Steve Peers and Sacha Prechal, "Article 52—Scope and Interpretation of Rights and Principles", in: Peers et al. (n 65), at para. 52.39 (Kindle edition),

[109] Ibid., at para. 52.42. See in this regard ibid., para. 52.44, and the Opinion of Advocate General Leger in Joined Cases C-317/04 and C-318/04 European Parliament v. Council and Commission, ECLI:EU:C:2005:710, paras. 216-221.

[110] The Ombudsman is to be US Under Secretary of State Catherine Novelli. See Annex III, Letter from US Secretary of State John Kerry (n 16).

[111] Commission v. Germany, Case C-518/07, 9 March 2010, ECLI:EU:C:2010:125, para. 19. See Herke Kranenbourg, "Article 8—Protection of Personal Data", in: Peers et al. (n 65), at para. 08.146.

standards for ombudsmen.[112]

--The Privacy Shield has a complex structure for resolution of complaints by individuals, which includes lodging a complaint with a member company; taking it to their national DPA; using an alternative dispute resolution mechanism; and, as a last resort, appealing to the "Privacy Shield Panel", which seems to be a kind of arbitration body. Article 47 of the Charter requires that an individual whose rights are violated have an "effective remedy before a tribunal", and in *Schrems* the CJEU held 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".[113] This suggests that the Court may take a dim view of complaint systems that do not involve a court, or those that place too much emphasis on dispute resolution by US entities not subject to control under EU law. On the other hand, the Court also found that "recourse by a third country to 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",[114] suggesting that it may be willing to take a more flexible view.

IV. Effect on other data transfer mechanisms

A. Introduction

The rule of law requires the consistent application of legal rules to similar situations,[115] and the CJEU strives to insure that its judgments enjoy legitimacy based on criteria such as coherency with existing case law, predictability, and avoidance of arbitrariness.[116] It is therefore important to look beyond the Safe Harbour and investigate the implications of the *Schrems* judgment on the other mechanisms in the Directive that may be used to create a legal basis for data transfers.

The criticisms made of the Safe Harbour by the Court can be applied by analogy to the other legal bases for data transfer under the Directive, and thus raise questions about their continued viability. The broader applicability of the judgment will be demonstrated with regard to the three sets of legal bases for data transfers set forth in Articles 25 and 26 of the Directive, namely adequacy decisions issued by the European Commission (Article 25), derogations (Article 26(1)), and "adequate safeguards" (Article 26(2)).

B. Adequacy decisions of the Commission

---

[112] Letter of European Ombudsman Emily O'Reilly to European Commissioner Věra Jourová, 22 February 2016, <http://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark>.
[113] *Schrems* (n 3), para. 95.
[114] Ibid. para. 81.
[115] Gunnar Beck, *The Legal Reasoning of the Court of Justice of the EU* (Hart Publishing 2012), at 234 (Kindle edition).
[116] See Koen Lenaerts, "How the ECJ Thinks: A Study on Judicial Legitimacy", 36 Fordham International Law Journal 1302, 1306 (2013).

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. 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.[117] These criteria must be applied to other adequacy decisions as well, which raises questions about their continued viability.

In particular, the same points made by the Court concerning access to data by the US intelligence services could be raised concerning several other adequacy decisions. Two of the countries that participate in the international "Five Eyes"[118] intelligence sharing network, which includes the United States, have also been found adequate by the Commission (i.e., Canada[119] and New Zealand[120]). 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",[121] that there was a "'significant over-reach' on the part of the NSA and other federal agencies",[122] and that in the US there has been "indiscriminate surveillance and interception carried out by them on a large scale".[123] In light of these findings, it seems that, at the least, explanation is required as to how countries that have deep and longstanding intelligence-sharing arrangements with the US can provide a level of data protection that is "essentially equivalent" to that under EU law.[124]

The Privacy Shield forms the basis of a proposed adequacy decision of the Commission.[125] As explained above, the Shield presents a number of legal questions that will likely have to be answered eventually by the CJEU. Such a judgment of the Court would also provide clarification on the extent to which the factors discussed in *Schrems* would apply to adequacy decisions of other countries as well.

---

[117] See, e.g., *Schrems* (n 3), para. 78 (stating "review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict").

[118] See regarding the Five Eyes alliance (which comprises Australia, Canada, New Zealand, the UK, and the US) Greenwald (n 54), at locations 1581, 1854-1900 (Kindle edition).

[119] See Commission Decision (EC) 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] OJ L2/13; 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] OJ L91/49.

[120] 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] OJ L28/12.

[121] *Schrems* (n 3), para. 11.

[122] Ibid., para. 30.

[123] Ibid., para. 31.

[124] This question could be asked of other countries that have been found by the Commission to provide adequate protection and that have strong national security states, for example Israel (European Commission, Commission Decision 2011/61/EU 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] OJ L27/39)). See Greenwald (n 54), at location 1904 (Kindle edition), 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".

[125] Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the E.U.-U.S. Privacy Shield (n 16).

C. Derogations

Article 26(1) of the Directive includes derogations for the restrictions on data transfers to third countries. 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 defence 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 "the 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)).

In its press release responding to the *Schrems* judgment, the European Commission noted that these derogations may still be used for data transfers,[126] which is correct in a formal legal sense, since they were not at issue in the judgment. However, the justification for relying on the derogations is undermined by the judgment.

By definition, the derogations are to be used in situations where there is no adequate level of data protection in the country to which the data are to be transferred,[127] and they must be applied narrowly.[128] The Article 29 Working Party has made it clear that in particular, consent cannot generally provide a long-term framework for "repeated or structural data transfers" (i.e., for repeated and large-scale transfers).[129] Thus, the derogations cannot fully replace the Safe Harbour as a means to conduct large-scale data transfers.

Moreover, since they are to be used in situations where no adequate data protection exists, use of the derogations does not address the issues with intelligence surveillance that caused the CJEU to invalidate the Safe Harbour. For example, it is self-evident that the fact that an individual has consented to a data transfer, or that the transfer is necessary to perform a contract, can provide no protection against data access by intelligence services. Therefore, while they remain valid in a formal legal sense, the derogations are subject to the same

---

[126] European Commission, "First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour" (n 7).

[127] See Article 26(1) of the Directive (n 2), 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)…"

[128] See 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, 24 July 1998), at 24, stating "These exemptions, which are tightly drawn, for the most part concern cases where risks to the data subject are relatively small or where other interests…override the data subject's right to privacy. As exemptions from a general principle, they must be interpreted restrictively".

[129] 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, 25 November 2005), at 11.

criticisms concerning intelligence surveillance that resulted in the invalidation of the Safe Harbour.

D. Adequate safeguards

The final possibility to provide a legal basis for data transfers is through the use of so-called "adequate safeguards". Article 26(2) of the Directive provides that transfers may be carried out absent adequate protection in the third country to which 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". In practice, two types of "adequate safeguards" are recognized, namely (1) contractual clauses, or (2) so-called binding corporate rules (BCRs). Contractual clauses are concluded between the data exporter in the EU and the party outside the EU to whom the data are sent, and contain obligations on each to provide certain protections to the data. They can either be "standard contractual clauses", the text of which is standardized and adopted by a formal decision of the European Commission,[130] or "ad hoc" clauses that are drafted in each specific case and may need to be approved by the DPAs before use.[131] Binding corporate rules 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.[132]

As is the case with derogations under Article 26(1), adequate safeguards under Article 26(2) were not at issue in the *Schrems* case, so that in a formal legal sense they remain valid.[133] This is brought out in a Communication on the judgment issued by the European Commission in November 2015,[134] in which it emphasized that other data transfer mechanisms under the Directive may still be used, such as derogations (e.g., consent) under Article 26(1) of the Directive, and adequate safeguards (i.e., binding corporate rules or standard contractual clauses) under Article 26(2).

However, adequate safeguards suffer from the same defects as does the Safe Harbour with regard to intelligence surveillance by third countries. In the first place, it is clear that a contractual agreement between two private parties, or a binding set of data protection rules within a corporate group, can not legally restrain government intelligence activities of third countries. Moreover, in a practical sense, the powers of intelligence services to access data

---

[130] 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>.

[131] See regarding the use of contractual clauses to transfer data Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press, 2007), at 191-208.

[132] See regarding BCRs Lokke Moerel, Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers (Oxford University Press 2012).

[133] This was mentioned in the Commission press release issued post-*Schrems*. See European Commission, "First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour" (n 7).

[134] European Commission, "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, 6 November 2015.

far exceed any protections that can be granted by paper-based protections such as contracts or compliance policies.

In his submission to the CJEU, Schrems implied that use of the standard contractual clauses results in a higher level of protection than does the Safe Harbour, since transfers under the clauses are "under supervision by DPAs".[135] However, not all Member States require that the standard clauses be filed with the DPAs.[136] Under the GDPR, the use of the standard clauses does not require DPA authorisation.[137] In addition, under the Directive, the DPAs' statutory enforcement powers end at their national borders,[138] so there is no way for them to enforce EU law with regard to data processing by foreign intelligence services. While the standard contractual clauses do include provisions giving the DPAs rights with regard to data importers in third countries,[139] they cannot allow the DPAs to exercise their statutory powers in third countries, nor do they have any powers against public authorities in third countries (such as intelligence services). Thus, the argument that the use of adequate safeguards provides added protection because of DPA involvement is essentially a legal fiction. Schrems apparently has come to change his views about the standard clauses, since in December 2015 he filed complaints against Facebook with DPAs in Belgium, Germany, and Ireland that attacked the use by the company of contractual clauses to transfer personal data.[140] Some DPAs have also raised questions about the use of adequate safeguards in light of the *Schrems* judgment.[141]

Neither the standard clauses nor BCRs provide legal protection against data access by foreign law enforcement. The standard contractual clauses allow for suspension of data flows by the DPAs when "it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection

[135] See Maximilian Schrems v. Data Protection Commissioner, Written Submissions of Applicant, <http://www.europe-v-facebook.org/CJEU_subs.pdf>, at 24.

[136] 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, 24 November 2014), at 2, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf>.

[137] See Article 42(2) of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21).

[138] EU Data Protection Directive (n 2), Article 28(6). See also *Weltimmo*, Case C-230/14, 1 October 2015, para. 60.

[139] E.g., Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46/EC of the European Parliament and of the Council, [2010] OJ L39/5, Clause 8, which gives DPAs the right to conduct an audit of the data importer.

[140] See <http://www.europe-v-facebook.org/EN/Complaints/PRISM_2_0/prism_2_0.html>.

[141] See "ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14', 14 October 2015, <https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-PositionPapier-on-CJEU_EN.pdf>, at 4, in which the data protection authority of the German federal state of Schleswig-Holstein stated "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."

law and the standard contractual clauses",[142] and provide for notification of data access to the data exporter.[143] Binding corporate rules must contain a commitment that when a member of the corporate group has reason to believe that the law applicable to it prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by them, it will inform the EU headquarters or the EU member with delegated data protection responsibilities (except where prohibited by criminal law), and that when there is conflict between national law and the commitments in the BCR, the company must "take a responsible decision on what action to take" and consult the competent DPAs in case of doubt.[144] Informing other members of the company or the DPAs about conflicts with third country law can by itself provide no protection to data processing, and DPAs can take no action to do so besides blocking data transfers outside the EU, which does not provide effective protection on a large scale and raises legal issues of its own.

E. The GDPR

It seems that the GDPR will take effect some time in 2018, at which time it will replace the Directive. The question thus arises of what effect it will have on data transfers in light of the *Schrems* judgment.

The GDPR includes a much more detailed definition of what constitutes "adequacy" for data transfers to third countries, which incorporates the standards adopted by the CJEU in *Schrems*.[145] Thus, entry into force of the GDPR will not change the situation regarding the standards for adequacy that the Court adopted. The GDPR retains the three major grounds for data transfers under the Directive, namely adequacy decisions,[146] derogations,[147] and appropriate safeguards[148] (the new designation for "adequate safeguards" under Article 26 of the Directive). It makes a number of changes to the legal framework, including explicit recognition of binding corporate rules,[149] the possibility of transferring data on a limited basis based on a "compelling legitimate interest of the data controller",[150] the possibility for EU law or Member State law to set limits for transfers of specific categories of personal data,[151] and the potential use of codes of conduct to transfer personal data.[152] There is also a new provision with rules regarding requests for disclosure of data by third country courts and administrative authorities.[153]

---

[142] See, e.g., Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors (n 139), Article 4(1).
[143] Id., Clauses 5(b) and 5(d).
[144] See Article 29 Working Party, "Working Document setting up a framework for the structure of Binding Corporate Rules" (WP 154, 25 June 2008), at 8.
[145] Article 41 and Recitals 81 and 81b of the GDPR version adopted by the Council and European Parliament on 15 December 2015 (n 21).
[146] Ibid., Article 41.
[147] Ibid., Article 44.
[148] Ibid., Article 42.
[149] Ibid., Article 43.
[150] Ibid., Article 44(1)(h).
[151] Ibid., Article 44(5)(a).
[152] Ibid., Article 38.
[153] Ibid. Article 43a, providing: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal

None of the changes implemented by the GDPR affect the points made here concerning the consequences of the *Schrems* judgment for regulation of international data transfers. In addition, the GDPR incorporates the standards of the *Schrems* judgment. Thus, the arguments made here will remain relevant once the GDPR enters into force.

V. Reactions to the judgment

The predominant reactions to the *Schrems* judgment prior to the issuance have focused on what I will call formalism (of which the Privacy Shield proposal is another example) and data localization. As will be seen, neither of these is sufficient to provide real protection for international data transfers. This strengthens the conclusion that regulation of international data transfers under EU data protection law often represents illusion more than reality.

A. Formalism

A formalistic approach attempts to protect international data transfers through the implementation of procedural safeguards. Regulation of data transfers is filled with such safeguards, which include individuals clicking consent boxes on websites; signature of standard contractual clauses; formal approval of data transfers by DPAs; and formal determinations of the adequacy of third countries by the European Commission.

The Court in *Schrems* puts considerable emphasis on the fact that protections provided for 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 Union" (emphasis added).[154] This reflects case law of the European Court of Human Rights, which requires that remedies for data protection violations be effective in practice as well as in law,[155] as well as similar statements by the Article 29 Working Party.[156] Individuals in the EU whose data are being transferred internationally are interested in ensuring that their rights are protected in practice, as is indicated by the widespread concern among Europeans about misuse of their data online.[157] Like any fundamental right, data protection cannot be reduced to a set of formalistic or bureaucratic procedures if it is to have any meaning.

Access to data transferred under Safe Harbour by the US intelligence services was one of the main factors in the Court's judgment, as can be seen in its emphasis on the fact that the Safe

---

assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter".

[154] *Schrems* (n 3), para. 74. See also para. 39 (referring to the need for "effective and complete" protection), para. 41 (referring to the importance of ensuring the "effectiveness" of monitoring of compliance with the law by DPAs), and paras. 81, 89, 91, and 95 (in which the Court stresses the need for protection of the fundamental right to data protection to be "effective").

[155] See, e.g., *Rotaru v Romania* (2000) ECHR 191, at para. 67.

[156] 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, 24 July 1998), at 5, stating that "data protection rules only contribute to the protection of individuals if they are followed in practice".

[157] See Special Eurobarometer 431, Data Protection, June 2015, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf>, at 25.

Harbour principles can be limited by national security or law enforcement requirements,[158] the lack of limits mentioned in the Safe Harbour on data use under US law for national security purposes,[159] and the failure in the Safe Harbour to mention any legal protection dealing with US intelligence surveillance.[160] In light of this, one can only conclude that the judgment requires meaningful and effective protection against intelligence surveillance by third countries. However, it is self-evident that procedures such as checking consent boxes on online forms, signing contractual clauses, or having binding corporate rules approved by DPAs cannot restrain data access by foreign intelligence services. At a legal level, such third country agencies are not constrained by EU law, and at a practical level their capabilities are not in any way hindered by such procedural mechanisms.

EU data protection law is partially based on legal fictions. Thus, Member States are required to consider all other Member States as complying with fundamental rights law, and may not check whether they do so in a specific case, based on the principle of mutual trust under EU law.[161] A concrete application of this principle can be seen in Article 1 of the Directive, which provides that Member States may not restrict data transfers to other Member States based on the level of data protection they provide, so that, legally speaking, all Member States are presumed to offer an adequate level of data protection.[162] This situation has been affirmed by the CJEU, which has ruled several times that harmonisation of national data protection laws in the Member States is "generally complete".[163]

At the same time, in announcing its legislative reform package for data protection in 2012, the European Commission stated that existing rules do not provide the degree of harmonization required, and that in particular there is a substantial lack of harmonisation in important areas.[164] The EU Fundamental Rights Agency has also found substantial divergences in the powers of national DPAs.[165] The principle that data protection standards are uniform among the Member States is thus a legal fiction, and there is a gulf between the presumption of harmonisation among Member State laws and the reality on the ground. Of course, data protection law, like any form of law, must to some extent rely on formalistic procedures, which further important values such as predictability and impartiality of the law. The problem arises when formalism becomes an end in itself, which is particularly inappropriate when fundamental rights are at stake.

The proposed Privacy Shield is another example of formalistic responses to regulation of international data transfers. The procedure for approval of adequacy decisions by the

---

[158] *Schrems* (n 3), paras. 84-86.
[159] Ibid., para. 88.
[160] Ibid., para. 89.
[161] Opinion 2/13 of the Court, 18 December 2014, CLI:EU:C:2014:2454, para. 192.
[162] EU Data Protection Directive (n 2), Article 1, stating "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1."
[163] *Bodil Lindqvist*, Case C-101/01, [2003] ECR I-12971, at para. 96, stating "The harmonisation of those national laws…amounts to harmonisation which is generally complete"; *ASNEF*, Joined Cases C-468/10 and C-469/10, [2011] ECR I-12181, at para. 29, stating "Accordingly, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete."
[164] European Commission, "Safeguarding Privacy in a Connected World" (n 20), at 4-7.
[165] See European Union Agency for Fundamental Rights (n 43).

European Commission under the Directive has been criticized as inefficient,[166] untransparent,[167] and subject to influence based on political factors.[168] The ground-breaking *Schrems* judgment provided the opportunity for the EU to re-think its approach to reaching adequacy determinations, and to consider what mechanisms could actually lead to data protection in the real world of international data transfers, but instead it moved to negotiate an adequacy decision with little transparency or chance for public input. The result is a massive package that will be difficult for individuals or smaller companies to implement or even understand.

B. Data localization

The second response to *Schrems* has been based on what can be referred to as data localization, which includes measures or policies to encourage or require the storage of personal data inside the borders of the EU, so that there is no need for data transfers.[169] Incentives have been proposed to store the data of European companies on servers located within the EU,[170] and, as the European Commission noted in its Communication following the judgment,[171] a number of US-based companies have announced plans to store data in Europe.[172]

Locating data storage in a particular place is normally a decision made on business and technical considerations. However, following the *Schrems* judgment, it is important to investigate whether data localization in Europe can provide effective protection against data access by the intelligence services; the answer seems to be "no".

---

[166] See regarding problems with the EU system for reaching adequacy determinations Article 29 Working Party, "The Future of Privacy" (WP 168, 1 December 2009), at 10-11, stating that the process for reaching adequacy decisions should be "redesigned".

[167] See Kuner, *Transborder Data Flows and Data Privacy Law* (n 38), at 48.

[168] 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 "Ireland blocks EU data sharing with Israel", 8 July 2010, <http://jta.org/news/article/2010/07/08/2739965/ireland- backs-out-of-data-sharing-with-israel>. Israel later received an adequacy decision from the European Commission; see Commission Decision 2011/61/EU 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] OJ L27/39. Also, a failed bid for adequacy by Australia in the early 2000s caused tensions between that country and the EU.

[169] See generally regarding data localization Anupam Chander and Uyê P. Lê, "Data nationalism", 64 Emory Law Journal 677 (2015); Christopher Kuner, "Data nationalism and its discontents", 64 Emory Law Journal Online 2089 (2015), <http://law.emory.edu/elj/_documents/volumes/64/online/kuner.pdf>

[170] See "Atos CEO calls for 'Schengen for data'", <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*, 10 November 2013, <http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html>.

[171] European Commission, "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" (n 134), at 12.

[172] See, e.g., Murad Ahmed and Richard Waters, "Microsoft unveils German data plan to tackle US Internet spying", Financial Times, 11 November 2015, <http://www.ft.com/intl/cms/s/0/540a296e-87ff-11e5-9f8c-a8d619fa707c.html#axzz3vvmkIE7x>; Karlin Lillington, "Oracle keeps European data within its EU-based data centres", Irish Times, 28 October 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>.

It is obvious that not all data processing services can be located in the EU. Thus, expecting data processing to be located in the EU in order 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,[173] it seems clear that Europeans want to use such services and communicate with parties in third countries.

There are also legal limits to creating incentives or requirements to locate data processing in a particular place. Under both EU and international human rights law, individuals have a right to communicate and transfer data "regardless of frontiers",[174] suggesting that the ability to communicate across national borders is a necessary component of the right to freedom of expression.[175] The exact meaning of the phrase "regardless of frontiers" with regard to freedom of expression in international human rights instruments remains unclear, as it never seems to have been specifically clarified by UN human rights agencies or the European Court of Human Rights.[176] A logical interpretation of the phrase would seem to be that the right to communicate across borders is subject to the same conditions and restrictions as other components of the right to freedom of expression. For example, in General Comment No. 34, the UN Human Rights Committee has taken a restrictive view of the possibility for states to put conditions on freedom of expression online, noting that they can only be imposed insofar as they are compatible with paragraph 19(3) of the ICCRP.[177] Given that communication on the Internet has an inherent cross-border element, it would seem that this view of the Human Rights Committee has particular relevance to any restrictions placed on the right to communicate across borders. That is, such restrictions may be permissible, but only as provided for by law and in order to protect important public values.

It is also not clear how much protection in practice data localization can provide against access by intelligence agencies. Storing data on computers physically located in the EU Member States will remove them from the direct enforcement jurisdiction of third countries, since under international law public authorities may generally not enforce laws abroad without the consent of the relevant country.[178] It may also be easier for EU individuals to

[173] 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 Special Eurobarometer 431, Data Protection, June 2015, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf>, at 24.

[174] See Universal Declaration of Human Rights (1948), Article 19; International Covenant of Civil and Political Rights (ICCRP) (1966), Article 19(2); European Convention on Human Rights (1953), Article 10(1).

[175] In each of the three human rights conventions referred to above in n 174, the phrase "regardless of frontiers" is mention in the article dealing with freedom of opinion and of expression (i.e., in the articles cited therein).

[176] See, e.g., UN Human Rights Committee, "General Comment No. 34", UN Doc. CCPR/C/GC/34, 12 September 2011, which mentions once the phrase "regardless of frontiers" but offers no interpretation of what it means; Lorna Woods, "Article 11", in: Peers (et al.) (n 69), at 314, noting that there have been no cases brought as of yet regarding the territorial scope of the right to freedom of expression under Article 11 of the European Convention on Human Rights.

[177] General Comment No. 34 (n 176), para. 43. Article 19(3) of the ICCRP provides that the right to freedom of expression (including that across borders) may be subject to restrictions only as "provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals".

[178] See, e.g., Ian Brownlie, *Principles of Public International Law* (7th ed Oxford University Press 2008), at 309, stating "the governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter"; F A Mann, 'The Doctrine of Jurisdiction in

assert their data protection rights with regard to data stored in EU Member States, since EU law provides individuals and regulators with a framework that allows the assertion of rights between the Member States.[179] Some companies have begun constructing services that purport to provide stronger protection against data access based on the localization of data storage within the EU, though the efficacy of such claims remains untested.[180]

However, as the Snowden revelations have shown, there seems to be widespread data sharing going on between EU intelligence services and those of third countries, in particular the US services and those of the "Five Eyes" intelligence sharing network.[181] 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.[182]

Thus, there is strong evidence to suggest 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 it may 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 globally-networked nature of data processing. The factual record concerning data sharing between intelligence agencies is unclear and subject to controversy, so that it is difficult to know exactly how and to what extent data are being shared between particular agencies. But the available evidence gives reason to doubt that the place of data storage has a strong influence on the level of protection it receives in practice.

International Law' (1964) 111 *Recueil des Cours de l'Académie de Droit International* 9, reprinted in F A Mann, *Studies in International Law* (Clarendon Press Oxford 2008) , at 145-146.

[179] See, e.g., EU Data Protection Directive (n 2), Article 28(6), which obliges EU data protection authorities to cooperate with each other; Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2001] OJ L12/1, which allows court decisions from one EU Member State to be enforced in another Member State.

[180] See, e.g., Murad and Waters (n 172), regarding a plan by Microsoft to allow customers to store their data in Germany under facilties that are under the control of Deutsche Telekom, in order to protect them from legal access by US law enforcement authorities.

[181] See, e.g., Greenwald (n 54), at locations 1852-1926 (Kindle edition), 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; SPIEGEL Online, "Spying Close to Home: German Intelligence under Fire for NSA Cooperation", 24 April 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, 1 November 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.

[182] Greenwald (n 181), at location 1857 (Kindle edition), stating that the GCHQ is the "closest NSA ally". See also Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", 56 Harvard International Law Review 81, 126 (2015).

Specifically with regard to the US, certain constitutional protections do not apply to non-US individuals abroad,[183] so that moving data processing to the EU does not necessarily create extra protection under US law. US courts have also ruled that companies can be compelled to comply with orders from US authorities no matter where in the world the data are stored;[184] this issue is currently the subject of a legal challenge in the US courts involving a warrant issued by the US to access data held by Microsoft at its servers in Ireland.[185]

VI. Conclusions

A. Reality and illusion in data transfer regulation

The *Schrems* judgment demonstrates both the reality and the illusion of EU regulation of international data transfers. The Court's strong affirmation of data protection rights clarifies the application of the Charter to data transfers, and thus continues the reality of legal protections for data protection rights that were advanced in *Digital Rights Ireland* and other judgments.

At the same time, it shows how EU law maintains the "exalting illusion" of global protection of data transfers based on EU standards. The points upon which the Court relied to invalidate the Safe Harbour can be applied 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 not be workable in practice. While it seems clear that the Charter provides the measure of adequate protection for data transfers in most cases, the exemption of national security from EU competence may lead to gaps in protection. The judgment thus lays bare the internal contradictions of the regulation of data transfers under EU law, and shows how the unilateral application of EU law cannot provide effective protection in practice for data transfers to third countries.

B. The politics of international data transfers

---

[183] For example, the warrant clause of the Fourth Amendment. See *United States v. Verdugo-Urquidez*, 494 US 259, 271 (1990). See also Kai Raustiala, *Does the Constitution Follow the Flag?* (Oxford University Press 2011); José A. Cabranes, "Our Imperial Criminal Procedure: Problems in the Extraterritorial Application of US Constitutional Law", 118 Yale Law Journal 1660 (2009).

[184] See, e.g., *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) (affirming sanctions against the defendant for refusing to produce documents held abroad in response to a grand jury subpoena); *In re Marc Rich & Co., A.G.,* 707 F.2d 663 (2d Cir. 1983) (affirming a grand jury subpoena ordering the defendant to produce records held in Switzerland); *United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir. 1981) (affirming a summons from the Internal Revenue Service to produce tax records held in Switzerland); *United States v. Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080 (S.D.N.Y. 1984) (granting a motion to force the defendant to produce records held in Hong Kong).

[185] *In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation*, Memorandum and Order 13 Mag. 2814 (S.D.N.Y., US Magistrate Judge James C. Francis IV), 25 April 2014. At the time this article was written, the case was being appealed to the US Court of Appeals for the Second Circuit. See *Microsoft Corporation v. United States of America*, Case 14-2985-CV (Second Circuit). See regarding the case Ned Schultheis, "Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry", 9 Brooklyn Journal of Corporate, Financial and Commercial Law 661 (2014-2015); Case Note, "In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F Supp. 3d 466 (S.D.N.Y. 2014)", 128 Harvard Law Review 1019 (2014-2015).

One reason that regulation of international data transfers often provides only the illusion of protection is that the legal arguments made are only reflections of deep-seated political positions. This can be seen particularly in the EU-US relationship, where the legal positions of each side are determined by their underlying political beliefs.

Parties in the EU wants to have the US adopt an EU-style data protection framework[186] and to change its law.[187] For its part, the US side would like the EU to make it easier to transfer personal data internationally, both to further economic growth[188] and for reasons of US national security.[189] This has produced resentment in the EU about the extent of US lobbying on data protection,[190] and in the US about the EU trying to have it change its law.[191] The political nature of the transatlantic disagreement is shown by the fact that the EU-US Privacy Shield was only finalised by a last-minute agreement at the highest political level on a call between European Commission First Vice-President Frans Timmermans and US Vice-President John Kerry.[192]

Transatlantic political disagreements about data protection rights are to be expected, since "rights to do not exist as such—'fact-like'—outside the structures of political deliberation. They are not a limit but an effect of politics".[193] Legal disagreements that are essentially political arguments in disguise cannot provide a solution to clashes between different conceptions of data protection and privacy, since they are determined, as Koskiniemi states,

---

[186] See, e.g., Press Release of the Transatlantic Consumer Dialogue (TACD), <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 dozens of consumer organizations in both the EU and the US, with the majority being European.

[187] See "Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe)", 26 October 2015, <http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm>, in which EU Commissioner Jourová urged the US to pass the proposed Judicial Redress Act, which would grant enhanced rights to EU individuals to bring privacy-related claims in the US. The Act was signed into law by President Obama on 24 February 2016 (n 18).

[188] See, e.g., Robert D. Atkinson, "Don't just fix Safe Harbour, fix the data protection regulation", EurActiv, 18 December 2015, <http://www.euractiv.com/sections/digital/dont-just-fix-safe-harbour-fix-data-protection-regulation-320567>, in which the president of a Washington-based think-tank urges reform of EU data protection law in order to facilitate data flows.

[189] See, e.g., Stewart Baker, "Time to get serious about Europe's sabotage of US terror intelligence programs", Washington Post, 5 January 2016, <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/01/05/time-to-get-serious-about-europes-sabotage-of-us-terror-intelligence-programs/>.

[190] See, e.g., April Dembosky and James Fontanella-Kahn, "US tech groups criticized for EU lobbying", Financial Times, 4 February 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.com, 21 February 2012, <http://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/>.

[191] See, e.g., Katie Bo Williams, "Last-minute change to privacy bill adds tension to US-EU talks", The Hill, 28 January 2016, <http://thehill.com/policy/cybersecurity/267401-last-minute-change-to-privacy-bill-adds-tension-to-us-eu-negotiations>, quoting Member of the US House of Representatives John Cornyn as stating with regard to adoption by the US of the proposed Judicial Redress Act, which would give rights under the US Privacy Act to Europeans, "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 (n 18).

[192] Zoya Sheftalovich, "The phone call that saved safe harbor", Politico, 13 February 2016, <http://www.politico.eu/article/the-phone-call-that-saved-safe-harbor-john-kerry-frans-timmermans/>.

[193] Martti Koskeniemi, *The Politics of International Law* (Hart 2011), at location 4421 (Kindle edition).

"by policy choices that seem justifiable only by reference to alternative conceptions of the good society".[194] Neither the EU nor the US positions can be separated from their political priorities, and arguments about issues such as where to set the balance between protecting data transferred internationally and furthering economic growth and national security only lead back to the policy assumptions that underlie each position.[195] 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 legal framework, without realizing that there can be no legal solution short of one side adopting the other's framework.

C. The way forward

Former European Data Protection Supervisor Peter Hustinx has written 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".[196] But the *Schrems* judgment shows how EU data protection law leaves narrow room for accommodation with the data protection systems of third countries. EU law does not view data transfer regulation as a way to reach a reasonable accommodation between EU standards and those of other countries, but focuses on a unilateral assertion of EU values. It is thus unrealistic to imagine that there could be a single, overarching "solution" to disputes between the EU and third countries regarding the regulation of international data transfers such as were the issue in *Schrems*.

However, while legal instruments cannot provide a full solution, they may serve as a "gentle civilizer of social systems",[197] based on finding lines of compatibility and communication between different data protection systems. Protecting international data transfers is unlikely to be possible under rigid, formalistic mechanisms that are based on strict criteria under national or regional law (such as EU formal adequacy decisions issued by the European Commission or the signing of standard contractual clauses), or by measures of pure formalism that cannot provide real protection in practice (such as the use of consent clauses).

If one believes that EU data protection law cannot and should not shut itself off from other legal systems, and that EU individuals 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. Regulation of international data transfers is marked by legal pluralism and fragmentation,[198] and scholarly consideration of ways to

---

[194] Ibid., at location 3995 (Kindle edition). 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: J.H.H. Weiler, *The Constitution of Europe* (Cambridge University Press 1999), 102, 106, stating that "Human rights are almost invariably the expression of a compromise between competing social goods in the polity".

[195] See Koskeniemi (n 193), at location 3939 (Kindle edition).

[196] Peter Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf>

[197] Andreas Fischer-Lescano and Gunther Teubner, "Regime-Collisions: the Vain Search for Legal Unity in the Fragmentation of Global Law", 25 Michigan Journal of International Law 999, 1045 (2003).

[198] Kuner, *Transborder Data Flows and Data Privacy Law* (n 38), at 160-165.

manage these phenomena could be applied to data protection as well.[199] The Privacy Shield is an example of an attempt to build bridges between different legal systems of data protection that, if it is adopted and not subject to a successful legal challenge, could prove to be an innovative solution that may have significance for data flows from the EU to other regions as well. However, the EU needs to modernize and open up its working methods to allow such schemes to be commented on in public while they are being devised, rather than being negotiated in secret with third countries and then adopted hurriedly without proper debate.

The fact that the perspective one takes on many of the privacy disagreements between the EU and the US determines the amount of difference between them gives hope that they may be less intractable than they seem. For example, at first glance there is considerable difference between the EU position that fundamental rights apply to all human beings, and the fact that US constitutional protections do not apply to the activities of its intelligence services operating abroad.[200] However, viewed at a broader comparative level, it turns out that French constitutional protections also do not apply to the activities abroad of national intelligence services,[201] and that this may be the case under German law as well.[202] Historians of human rights such as Mony have also shown how until fairly recently even in European polities there was an "umbilical connection between rights and citizenship".[203] This illustrates how many questions of fundamental rights protection depend on the perspective of the observer: if one is determined to find differences and disagreements between the EU and the US, then it is easy to do so, while if one wants to find possibilities for agreement, then they can also be found.

Three points are crucial to a workable system of data transfer regulation in EU law. First, the EU must move beyond formalistic and political measures and legal fictions to implement

---

[199] See, e.g., Paul Schiff Berman, *Global Legal Pluralism* 152 (Cambridge University Press 2014), who mentions as possible mechanisms "dialectical legal interactions, margins of appreciation, limited autonomy regimes, subsidiarity schemes, hybrid participation arrangements, mutual recognition regimes, safe harbor agreements, and regime interaction".

[200] See on this point Christopher Kuner, "Foreign Nationals and Data Protection Law: A Transatlantic Analysis", in: *Data Protection 2014: How to Restore Trust* 213 (Hielke Hijmans and Herke Kranenbourg eds.) (intersentia 2014)

[201] Assemblee Nationale, "Rapport d'information déposé en application de l'article 145 du Règlement par la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement", 14 May 2013, at <http://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf>. See also Winston Maxwell, "The legal framework for access to data by French law enforcement and intelligence agencies", (2014) 4 International Data Privacy Law 4, at 9, noting that, according to French newspaper reports, "France's intelligence agencies take the position that their collection of data outside of France does not fall under French legal constraint".

[202] *Compare* Bethold Huber, "Die Strategische Rasterfahndung des Bundesnachrichtendiestes – Eingriffsbefugnisse und Regelungsdefizite", (2013) 35 *Neue Juristische Wochenschrift* 2576, who finds that in theory the Basic Law does apply in such situations but criticizes the failure to implement such protections in legislation governing the intelligence services, *with* an interview with Prof. Dr. Christoph Gusy ("Die BND-Auslandsaufklärung im rechtsfreien Raum", 2 September 2013, <http://www.golem.de/news/datenueberwachung-die-bnd-auslandsaufklaerung-im-rechtsfreien-raum-1309-101324.html>), who states that surveillance of non-Germans outside Germany by the intelligence services is not covered by the Basic Law.

[203] Samuel Mony, *The Last Utopia: Human Rights in History* (Harvard University Press 2010), location 444 (Kindle edition).

actual protection in practice. Second, it must discard illusions, such as the idea that DPAs and national courts can perform meaningful assessments of the adequacy of non-EU data protection systems. Third, 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. In particular, it is necessary for the Court or the EU legislator to clarify the application of data protection rights under the Charter to situations involving national security, in order to remove any gaps in protection.

The *Schrems* judgment forces us to look at the contradictions of EU data transfer regulation squarely in the face. It is no longer possible to ignore the legal and logical incoherency of EU data transfer regulation, or to pretend that they can be cured by formalistic measures. Perhaps the common deficiencies in the legal systems of data protection in both sides of the transatlantic debate can provide common ground to overcome the illusions of the current data protection debate, and to bring the discussion back to reality.