Boston College International and Comparative Law Review

Volume 40
Issue 3 *Electronic Supplement*

Article 1

4-19-2017

Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in *Schrems v. Irish Data Protection Commissioner*

Christina Lam
Boston College Law School, christina.lam@bc.edu

UNSAFE HARBOR: THE EUROPEAN UNION'S DEMAND FOR HEIGHTENED DATA PRIVACY STANDARDS IN *SCHREMS v. IRISH DATA PROTECTION COMMISSIONER*

CHRISTINA LAM*

Abstract: In 1995, the European Union adopted the Data Protection Directive to govern the processing, use, and exchange of personal data. The United States refused to enact similar legislation, consequently jeopardizing ongoing and future data transfers with the European Union. To prevent economic catastrophe, the United States negotiated with the European Union to reach the Safe Harbor Agreement and, on July 26, 2000, the European Commission formally recognized the agreement as compliant with the Data Protection Directive in its Safe Harbor Decision. In 2013, U.S. data protection standards were once again placed under the microscope when Edward Snowden leaked information regarding the National Security Agency's surveillance activities. In the wake of these leaks, Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner, claiming that Facebook was not adequately protecting his personal data from National Security Agency surveillance when transferring it from its European Union servers to its U.S. servers. On October 6, 2015, the European Court of Justice invalidated the Safe Harbor Decision in *Schrems v. Irish Data Protection Commissioner.* This Comment examines the court's reasoning and argues that the court erred in interpreting Article 25 of the Data Protection Directive and overstepped jurisdictional boundaries.

INTRODUCTION

Both the United States and European Union (EU) avow a commitment to protecting data privacy, but their drastically different approaches have repeatedly been a source of tension.[1] In 1995, the EU adopted the Data Protection Directive (DPD) as a comprehensive regulatory framework for processing, using, and exchanging personal data.[2] The United States remained resistant to similarly standardizing its data protection practices, threatening the continuance of data trans-

* Christina Lam is a Staff Writer for the *Boston College International & Comparative Law Review*.

[1] *See, e.g.*, MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1–2 (2016); Lee A. Bygrave, *Transatlantic Tensions on Data Privacy* 3–4, 6 (Transworld, Working Paper No. 19, 2013).

[2] *See, e.g.*, WEISS & ARCHICK, *supra* note 1, at 2; Lucas Bergkamp, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER L. & SECURITY REV. 31, 32–33 (2002).

fers between the EU and the United States.[3] Under considerable pressure, the United States negotiated with the EU to reach the Safe Harbor Agreement and, on July 26, 2000, the European Commission (Commission) recognized the agreement as compliant with the DPD in its Safe Harbor Decision (Safe Harbor).[4] In 2013, U.S. data protection standards were, once again, a matter of controversy when Edward Snowden exposed the U.S. National Security Agency's (NSA) extensive surveillance activities.[5] Ultimately, on October 6, 2015, the European Court of Justice (ECJ) found that the United States provided an inadequate level of data protection and invalidated Safe Harbor in *Schrems v. Irish Data Protection Commissioner*.[6] This decision aroused uncertainty for an estimated 4500 U.S. companies and organizations that had been relying on Safe Harbor to legally carry out data transfers.[7]

Part I of this Comment provides a brief background of Safe Harbor and its invalidation in *Schrems v. Irish Data Protection Commissioner*. Part II delivers a discussion of the relevant EU law, the arguments presented, and the court's decision. Part III analyzes the decision's importance and its implications for U.S. data privacy law. This Comment contends that the court misconstrued the term "adequate" in Article 25 of the DPD and invaded the jurisdictional province of the United States and all other countries outside of the EU.

I. BACKGROUND

A. The Origins of Safe Harbor

The EU's lingering animosity towards past fascist and totalitarian policies of complete governmental control has inspired an ongoing campaign for personal data privacy.[8] As part of that campaign, the EU adopted the DPD in 1995 to "ensure a high level of protection for the privacy of individuals in all member

---

[3] *See* WEISS & ARCHICK, *supra* note 1, at 5; Bygrave, *supra* note 1, at 7, 9.

[4] *See* Commission Decision 2000/520 of July 26, 2000, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7, 8 (EC); WEISS & ARCHICK, *supra* note 1, at 5.

[5] *See* WEISS & ARCHICK, *supra* note 1, at 8–9.

[6] *See* C-362/14, Schrems v. Irish Data Prot. Comm'r, 2015 E.C.R. I-650, ¶ 106; WEISS & ARCHICK, *supra* note 1, at 6.

[7] *See* WEISS & ARCHICK, *supra* note 1, at 6; Noëlle Lenoir, *The Trouble with* Schrems, PROJECT SYNDICATE (Feb. 9, 2016), https://www.project-syndicate.org/commentary/safe-harbor-troubles-max-shrems-by-noelle-lenoir-2016-02 [https://perma.cc/93BW-G4GC].

[8] Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) ("[T]otalitarian regimes in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control. Even without computers, these regimes demonstrated the fragility of the human capacity for self-determination in the face of widespread spying and data collection."); *see* WEISS & ARCHICK, *supra* note 1, at 2; Bergkamp, *supra* note 2, at 32.

states . . . and also to help ensure the free flow of information society services in the [EU] by fostering consumer confidence and minimizing differences between the Member States' rules."[9] The DPD subjects nearly all data collection, usage, and transfers to a wide range of regulations and requires each EU member state to have at least one independent, data protection authority to monitor compliance.[10]

Under Article 25 of the DPD, transfers of personal data to non-European Economic Area countries (third countries) are only allowed if that country ensures an adequate level of data protection.[11] Such data transfers between the EU and third countries have become commonplace with the rise of the global economy and the unbounded nature of the Internet.[12] For example, EU companies routinely transfer and receive data from companies in third countries when seeking digitally deliverable services such as consulting, architecture, design, and finance.[13]

Both EU and U.S. government officials recognized that U.S. data protection standards were likely far too different from the DPD to be considered "adequate."[14] As a result, the United States entered into negotiations with the EU, leading the U.S. Department of Commerce to issue the Safe Harbor Privacy Principles in 2000.[15] Shortly thereafter, the Commission recognized the Safe Harbor Privacy Principles as ensuring an adequate level of data protection in its Safe Harbor Decision.[16] Under Safe Harbor, a U.S. company or organization could legally participate in data transfers with the EU as long as it annually self-certified to the U.S. Department of Commerce that it had complied with certain

---

[9] Colin J. Bennett & Charles D. Raab, *The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response*, 13 INFO. SOC'Y 245, 249 (1997) (quoting European Commission Press Release IP/95/822, Council Definitively Adopts Directive on Protection of Personal Data (July 25, 1995)).

[10] *See* Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, arts. 3, 28, 1995 O.J. (L 281) 39, 47 (EC) [hereinafter Data Protection Directive].

[11] *Id.* art. 25.

[12] *See* Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* 10–11 (Global Economy & Development, Working Paper No. 79, 2014) (estimating that economic activity that relies on transatlantic data flows accounts for forty percent of U.S. exports to the European Union (EU) and fifty-two percent of exports from the EU to the United States).

[13] *See id.* at 12.

[14] *See* WEISS & ARCHICK, *supra* note 1, at 5; Bygrave, *supra* note 1, at 9. The Data Protection Directive (DPD) serves as an individual, comprehensive framework for protecting data across the EU. *See* WEISS & ARCHICK, *supra* note 1, at 2. In contrast, the United States has taken a piecemeal approach to data protection. *See* WEISS & ARCHICK, *supra* note 1, at 3. For instance, the U.S. Privacy Act of 1974 regulates personal data under the government's control and an entirely separate law—the Electronic Communications Privacy Act of 1986—prevents the government from obtaining personal data sent from computers. *See* WEISS & ARCHICK, *supra* note 1, at 3.

[15] WEISS & ARCHICK, *supra* note 1, at 5.

[16] Commission Decision 2000/520, *supra* note 4; WEISS & ARCHICK, *supra* note 1, at 5.

principles and requirements regarding notice, choice, onward transfers, security, data integrity, access, and enforcement.[17]

B. The End of Safe Harbor

On June 25, 2013, Austrian national Maximillian Schrems brought a complaint to the Irish Data Protection Commissioner (Commissioner) that, in light of leaked information regarding U.S. intelligence activities, Facebook's EU-based servers in Ireland did not adequately protect the transfer of his data to its U.S. servers.[18] Specifically, Schrems claimed that Facebook could not possibly have transferred his personal data in accordance with EU law because the NSA had been intercepting those transfers.[19] The Commissioner refused to investigate Schrems' complaint, taking the position that Facebook adhered to Safe Harbor and therefore provided an adequate level of data protection.[20] The Commissioner further held that Schrems lacked evidence that the NSA had, in fact, accessed his personal data.[21] Schrems appealed the Commissioner's decision to the Irish High Court, which subsequently stayed the proceedings and submitted the case to the ECJ on July 17, 2014.[22]

II. DISCUSSION

A. Questions Before the Court

The Irish High Court asked the ECJ to consider two main questions in *Schrems*.[23] The first was whether an existing Commission finding of adequacy

---

[17] *See* Commission Decision 2000/520, *supra* note 4, annex I, at 11–12; WEISS & ARCHICK, *supra* note 1, at 5–6. The European Commission's Safe Harbor Decision (Safe Harbor) was an easy and cost-effective mechanism for complying with the DPD, but not the only mechanism. *See* Brian J. McGinnis & Brendan W. Miller, *European Court of Justice Invalidates U.S.-EU Safe Harbor Agreement*, NAT'L L. REV. (Oct. 9, 2015), http://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safe-harbor-agreement [https://perma.cc/G5EM-6ZRC]. Alternative mechanisms include model contract clauses and binding corporate resolutions. McGinnis & Miller, *supra*.

[18] *Schrems*, 2015 E.C.R. ¶¶ 26, 28. In 2013, Edward Snowden revealed that the National Security Agency (NSA) engaged in "upstream" collection, meaning it was intercepting Internet and telephone communications in and out of the United States on a "massive scale." Jenna McLaughlin, *Top European Court Rules That NSA Spying Makes U.S. Unsafe for Data*, INTERCEPT (Oct. 6, 2015), https://theintercept.com/2015/10/06/top-european-court-rules-that-nsa-spying-makes-u-s-unsafe-for-data/ [https://perma.cc/SSV6-YFA9]. The NSA also collected communications of "targeted individuals" by way of the PRISM program. McLaughlin, *supra*.

[19] McLaughlin, *supra* note 18.

[20] *See Schrems*, 2015 E.C.R. ¶ 29; WEISS & ARCHICK, *supra* note 1, at 6.

[21] *Schrems*, 2015 E.C.R. ¶ 29.

[22] *Id.* ¶¶ 30, 36.

[23] C-362/14, Schrems v. Irish Data Prot. Comm'r, 2015 E.C.R. I-650, ¶ 36. The Irish High Court referred the following questions to the European Court of Justice for a preliminary ruling:

> (1) Whether in the course of determining a complaint which has been made to [the Commissioner] that personal data is being transferred to another third country . . . the

binds the Commissioner when investigating a complaint.[24] The second was whether the Commissioner had the authority or was required to conduct an investigation based on factual developments that had occurred in the time since the adequacy finding was made.[25] Beyond the Irish High Court's two questions, the ECJ also considered the broader issue of whether Safe Harbor was consistent with EU law.[26]

B. Relevant Law

In reaching its findings, the ECJ primarily relied on Articles 25 and 28 of the DPD as well as Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union (EU Charter).[27] Article 25 of the DPD provides that data transfers to third countries are only permitted if that country ensures an adequate level of data protection and the Commission is allowed to issue findings of adequacy.[28] Article 28 of the DPD requires member states to set up at least one public authority to monitor compliance.[29] Articles 7, 8, and 47 of the EU Charter protect individual rights to privacy, data protection, and an effective remedy and fair trial, respectively.[30]

C. Arguments

Schrems, along with the European Parliament, a number of member states, and Digital Rights Ireland, maintained that U.S. mass surveillance practices were incompatible with privacy and data protection rights guaranteed under the DPD and the EU Charter.[31] Accordingly, Schrems claimed that his individual rights

---

> laws and practices of which, it is claimed, do not contain adequate protections for the data subject, [the Commissioner] is absolutely bound by the Community finding to the contrary contained in [the Safe Harbor Decision] 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 [Commissioner] conduct his or her own investigation of the matter in the light of factual developments in the meantime since [Commission Decision 2000/520] was first published?

Id.

[24] *Id.*

[25] *Id.*

[26] *See id.* ¶ 67.

[27] *Id.* ¶ 1.

[28] Data Protection Directive, *supra* note 10, art. 25.

[29] *Id.* art. 28.

[30] Charter of Fundamental Rights of the European Union, arts. 7–8, 47, 2000 O.J. (C 364) 10, 20.

[31] McLaughlin, *supra* note 18; Sam Schechner & Valentina Pop, *Personal Data Gets Day in Court*: *Safe Harbor Agreement Allows Transfer of Personal Information from Europe to the U.S.*, WALL ST. J. (Mar. 24, 2015, 3:58 PM), http://www.wsj.com/articles/court-hears-challenge-to-safe-harbor-data-deal-1427206554 [https://perma.cc/V637-68VX]; Sam Pfeifle, *ECJ Hears Safe Harbor*

were violated even though he was unable to prove that the NSA retrieved his personal data.[32] The Commissioner and the Commission admitted that Safe Harbor was flawed, but countered that the framework was too politically and economically necessary to invalidate.[33] The Commission gave assurance that Safe Harbor was still under negotiation and recommended a thirteen-point plan for its reform.[34] The Commissioner and Commission argued that, given Safe Harbor's extreme importance, the ECJ should allow it to stand in the interim.[35]

D. The Court's Holding

In response to the first question posed, the ECJ answered in the negative, holding that Safe Harbor does not prohibit the Commissioner and other national Data Protection Agencies (DPAs) from investigating and assessing data transfers with third countries.[36] The ECJ found that DPAs "must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him."[37] Although the ECJ recognized that DPAs have a significant amount of authority, only the court has the authority to invalidate Commission decisions.[38]

After identifying the court and Commissioner's authority, the ECJ assessed Safe Harbor, ultimately finding it invalid.[39] The ECJ interpreted the term "adequate level of protection" in Article 25 of the DPD to require third countries to provide "a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union by virtue of . . . [the DPD] read in light of the [EU] Charter."[40] The ECJ found that Safe Harbor did not meet the essentially equivalent requirement because it allowed the United States to disregard Safe Harbor principles when in conflict with national security, public interest, and law enforcement requirements, thereby undermining the fundamental right to privacy under Article 7 of the EU Charter.[41]

The court also held that Safe Harbor was in conflict with Article 47 of the EU Charter because it did not refer to the existence of U.S. rules or legal protections intended to limit U.S. interference with data privacy, such as an effective

---

Arguments, IAPP: THE PRIVACY ADVISOR (Mar. 24, 2015), https://iapp.org/news/a/ECJ-hears-safe-harbor-arguments/ [https://perma.cc/NP8N-F6CM].

[32] *See* Schechner & Pop, *supra* note 31.

[33] *See* Pfeifle, *supra* note 31.

[34] *Id.*

[35] *Id.*

[36] *See Schrems*, 2015 E.C.R. ¶ 43.

[37] *Id.* ¶ 99.

[38] *See id.* ¶ 62.

[39] *Id.* ¶¶ 100–103, 106.

[40] *Id.* ¶ 73 (emphasis added).

[41] *Id.* ¶¶ 73, 86–87.

judicial remedy.[42] Rather, the system of self-certification, in which a company declares it will follow the Safe Harbor principles, would only be a reliable measure of adequacy if there were mechanisms in place to identify and reprimand non-compliant U.S. companies.[43] The ECJ further found that, under Article 25 of the DPD, the Commission must evaluate a third country's domestic laws and international commitments prior to making a determination on the country's data protection standards.[44] However, the Commission did not evaluate U.S. laws and international commitments when issuing Safe Harbor.[45]

III. ANALYSIS

Immediately after the ECJ issued its decision in *Schrems v. Irish Data Protection Commissioner*, the EU and the United States entered into negotiations to devise a suitable data protection framework to replace Safe Harbor.[46] On February 2, 2016, an agreement was officially reached on "Privacy Shield" and the Commission issued its adequacy finding on July 12, 2016.[47] Although Privacy Shield reflects the requirements that the ECJ set out in *Schrems*, these requirements were formulated on an erroneous and judicially imprudent interpretation of "adequate" under Article 25 of the DPD.[48] Even with Privacy Shield in effect, it is unlikely that the EU will see the desired reforms in U.S. intelligence practices.[49]

---

[42] *Id.* ¶¶ 81, 89, 95.

[43] *Id.* ¶¶ 81, 89.

[44] *Id.* ¶ 83.

[45] *Id.*

[46] Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems, 18 GERMAN L.J. (forthcoming 2017) (manuscript at 19–20), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346 [https://perma.cc/2WH6-9Q5T].

[47] European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016). *See generally* Letter from Penny Pritzker, U.S. Sec'y of Commerce, to Vêra Jourová, Comm'r for Justice, Consumers & Gender Equal., Eur. Comm'n (Feb. 23, 2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf [https://perma.cc/2NWS-TTWV]. Privacy Shield is a lengthened, more specific version of the Safe Harbor Privacy Principles. WEISS & ARCHICK, *supra* note 1, at 9; *see* Kuner, *supra* note 46, at 20. It contains requirements in the following categories: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability. WEISS & ARCHICK, *supra* note 1, at 9. Unlike Safe Harbor, Privacy Shield includes an arbitration model and commitments from U.S. national security officials. WEISS & ARCHICK, *supra* note 1, at 9, 10.

[48] *See* Data Protection Directive, *supra* note 10, art. 25; Kuner, *supra* note 46, at 17–18; Memorandum from Geoffrey Robertson, Doughty Street Chambers, to Facebook, ¶ 11 (Jan. 14, 2016), blogs.ft.com/brusselsblog/files/2016/01/Geoffrey-Robertson-QC.docx [https://perma.cc/25CG-GBZW] [hereinafter Memorandum from Geoffrey Robertson].

[49] *See* Kuner, *supra* note 46, at 4.

A. Defining Adequate

The ECJ conceded that the word "adequate" in Article 25 of the DPD does not require a third country to ensure a level of protection that is "identical" to that guaranteed under EU law.[50] Apart from this one sensible limitation, the court found itself at liberty to adopt almost any interpretation of "adequate," as the DPD does not provide a definition.[51] The ECJ chose a very narrow interpretation of "adequate": third countries must have data protection standards in place that are "essentially equivalent" to the EU standards.[52] The court's use of the word "essentially" before "equivalent" makes the standard seem somewhat less rigid than "identical."[53] Even so, the essentially equivalent standard suffers from the same pitfalls as the identical standard: the text and structure of the DPD do not support it and it is overly burdensome on third countries.[54]

The word "equivalent" is synonymous with the word "identical."[55] In adding the word "essentially," the ECJ made it clear that a third country's level of data protection does not need to be identical to what the DPD provides.[56] In English, "essentially" is defined as "relating to the most important characteristics or ideas of something."[57] Therefore, under the essentially equivalent standard, third countries are required to provide a level of protection that is basically the same or identical in central or primary respects as that guaranteed within the EU.[58]

The plain language of the DPD neither requires nor insinuates the ECJ's interpretation of "adequate."[59] In a non-binding opinion submitted to the ECJ, Advocate General Bot identifies the English meaning of the word "adequate" as "satisfactory or sufficient" and contrasts it with the French meaning of "adéquat"

---

[50] C-362/14, Schrems v. Irish Data Prot. Comm'r, 2015 E.C.R. I-650, ¶ 73; *see* Data Protection Directive, *supra* note 10, art. 25.

[51] *See Schrems*, 2015 E.C.R. ¶ 70.

[52] *Id.* ¶ 73; *see* Kuner, *supra* note 46, at 17.

[53] *See Schrems*, 2015 E.C.R. ¶ 73.

[54] *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 17–18, 24 (2012) (arguing that, in requiring third countries to provide an adequate level of data protection, the EU places unreasonable restraints on business practices and imposes a high cost of compliance); Kuner, *supra* note 46, at 17.

[55] *Equivalent*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/equivalent [https://perma.cc/2BE4-8A7X].

[56] *See Schrems*, 2015 E.C.R. ¶ 73.

[57] *Essentially*, CAMBRIDGE DICTIONARY, http://dictionary.cambridge.org/us/dictionary/english/essentially [https://perma.cc/MXA7-D5CF]. "Essentially" is the adverb form of "essential," which means "of, relating to, or constituting essence" and "of the upmost importance." *Essential*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/essential [https://perma.cc/TME4-VSWL].

[58] *See Schrems*, 2015 E.C.R. ¶ 73; *Equivalent*, *supra* note 55; *Essentially*, *supra* note 57.

[59] *See Schrems*, 2015 E.C.R. ¶ 73; Data Protection Directive, *supra* note 10, art. 25; Kuner, *supra* note 46, at 17.

which is "appropriate."[60] Even under the more generous French definition, "adequate" seems to imply a lesser standard than "essentially equivalent."[61] Given that the EU's data protection framework has been identified as the "most ambitious, comprehensive, and complex in the field," it is conceivable that a third country could be found to have a level of data protection that is "appropriate," but not close enough to what EU law provides to be considered "essentially equivalent."[62]

The essentially equivalent standard is not only contrary to the DPD's plain language, but also to its overall structure.[63] The DPD is very deferential to EU member states, imposing few requirements on their discretion in order to allow them to balance competing interests, such as economic relations and data privacy.[64] Accordingly, the European Parliament most likely left the language of Article 25 vague to allow the Commission to balance competing interests and allow data transfers to continue under a wide range of data protection laws.[65] The essentially equivalent standard, however, significantly reduces the Commission's discretion to issue findings of adequacy.[66] For example, if a third country does not provide a level of data protection close to what is guaranteed in the EU, the Commission cannot find the third country's data protection laws "adequate" even if such a finding will seriously jeopardize economic relations.[67]

---

[60] Opinion of Advocate General Bot, ¶ 142, *Schrems*, 2015 E.C.R. ¶ 142.

[61] *See id.*

[62] Bygrave, *supra* note 1, at 5; *see* Opinion of Advocate General Bot, *supra* note 60; Memorandum from Geoffrey Robertson, *supra* note 48. Without much additional explanation, Advocate General Bot concluded that "the only criterion that must guide the interpretation of [adequate] is the objective of attaining a high level of protection of fundamental rights." Opinion of Advocate General Bot, *supra* note 60. This objective has been argued to be "merely an aspiration" mentioned in the Preamble to the DPD. Memorandum from Geoffrey Robertson, *supra* note 48. Nevertheless, data protection laws may be "adequate" without affording a "high level" of protection. Memorandum from Geoffrey Robertson, *supra* note 48.

[63] *See Schrems*, 2015 E.C.R. ¶ 73; MARTON VARJU, EUROPEAN UNION HUMAN RIGHTS LAW: THE DYNAMICS OF INTERPRETATION AND CONTEXT 97–98 (2014); JACQUES BOURGEOIS ET AL., SIDLEY AUSTIN LLP, ESSENTIALLY EQUIVALENT: A COMPARISON OF THE LEGAL ORDERS FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND UNITED STATES 13 (2016); Bennett & Raab, *supra* note 9, at 252.

[64] VARJU, *supra* note 63; Bennett & Raab, *supra* note 9, at 252. In *Lindqvist*, the European Court of Justice demonstrated the balancing exercise involved in considering whether Lindqvist violated the DPD when she posted church volunteers' personal information on a website without their consent. *See* Case C-101/01, Lindqvist, 2003 E.C.R. I-12992, ¶¶ 12–14, 86. The court weighed "Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life . . . against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site." *Id.* ¶ 86.

[65] *See* VARJU, *supra* note 63; BOURGEOIS ET AL., *supra* note 63.

[66] *See Schrems*, 2015 E.C.R. ¶ 73; VARJU, *supra* note 63; BOURGEOIS ET AL., *supra* note 63, at 27.

[67] *See Schrems*, 2015 E.C.R. ¶ 73; BOURGEOIS ET AL., *supra* note 63. *But see* Bennett & Raab, *supra* note 9, at 254–55 (arguing that it is dangerous for Commission decisions on adequacy to be influenced by wider political and economic concerns that are unrelated to data privacy).

Perhaps the most problematic result of the ECJ's interpretation of "adequate" is its extraterritorial effect.[68] That is, the "attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law."[69] The international political system has historically been organized around the notion of equal sovereignty of states, meaning each state only has control over its territory.[70] Therefore, any exercise of extraterritorial jurisdiction undermines the international order.[71]

By requiring that third countries ensure a level of data protection that is very similar to what is provided in the EU, the ECJ has effectively dictated the rest of the world's data protection legislation.[72] Although essential equivalence is only required when a third country is involved in data transfers with the EU, it is often too technologically difficult or too costly to operate under multiple sets of data protection standards and to have to separate European from non-European data. [73] Consequently, many companies and organizations have adopted the standard used for EU data transfers as their global standard.[74]

The ECJ should not have adopted the essentially equivalent standard in interpreting Article 25 of the DPD.[75] Rather, the court should have interpreted "adequate" more broadly as "sufficient" or "satisfactory" in order to adhere to the spirit and text of the DPD and minimize the standard's burden on third countries.[76] Furthermore, the ECJ's interpretation of "adequate" ignored the reality that cultural values and policy preferences, such as robust national security, heavily influence a country's desired level of data protection.[77]

---

[68] *See Schrems*, 2015 E.C.R. ¶ 73; Kuner, *supra* note 46, at 10.

[69] Christopher Kuner, *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*, 5 INT'L DATA PRIVACY L. 235, 238 (2015) (quoting Int'l Law Comm'n, Rep. on the Work of Its Fifty-Eighth Session, U.N. Doc. A/61/10, at 229 (2006)).

[70] Jamie Scudder, *Territorial Integrity: Modern States and the International System*, EXPLORING GEOPOLITICS (2010), http://www.exploringgeopolitics.org/publication_scudder_jamie_territorial_integrity [https://perma.cc/ZE48-8SK9].

[71] *See id.*

[72] *See* Bradford, *supra* note 54, at 17–18; Kuner, *supra* note 46, at 10–11.

[73] Bradford, *supra* note 54, at 17–18; *see* Data Protection Directive, *supra* note 10, art. 25. The phenomenon of the EU externalizing its laws and regulations through market mechanisms is often referred to as "the Brussels Effect." Bradford, *supra* note 54, at 3.

[74] *See* Bradford, *supra* note 54, at 18, 24.

[75] *See Schrems*, 2015 E.C.R. ¶ 73; Data Protection Directive, *supra* note 10, art. 25; Kuner, *supra* note 46, at 17.

[76] *See Schrems*, 2015 E.C.R. ¶ 73; Opinion of Advocate General Bot, *supra* note 60; Data Protection Directive, *supra* note 10, art. 25; VARJU, *supra* note 63; Bradford, *supra* note 54, at 17–18.

[77] *See* Bygrave, *supra* note 1, at 7–9; Kuner, *supra* note 46, at 18.

B. The Balance Between Privacy and National Security

The ECJ cited many problems with Safe Harbor, but the decision to invalidate it hinged on the unrestricted nature of U.S. intelligence practices.[78] Admittedly, U.S. law and practice allow for large-scale data collection.[79] Even so, Safe Harbor's invalidation was not legally justified and the ECJ exceeded its jurisdictional authority in disallowing third countries from engaging in mass surveillance.[80]

The court found U.S. mass surveillance practices to be inconsistent with the right to private life under Article 7 of the EU Charter.[81] Although the EU Charter does not directly bind the United States, the ECJ interpreted Article 25 of the DPD to require third countries to provide a level of protection that is "essentially equivalent" to that provided in the DPD "read in light of the EU Charter."[82] The DPD therefore extraterritorially binds third countries to the EU Charter and places a "*per se* limit" on mass surveillance practices.[83] Even though the ECJ's decision was concerned with the mass surveillance of EU citizens, the nature of mass surveillance renders it impossible to confine its targets.[84] The court therefore effectively prohibits third countries from engaging in mass surveillance of both EU and non-EU citizens so long as they participate in data transfers with the EU.[85] However, such an interpretation is contrary to international custom; many countries other than the United States engage in mass surveillance practices, including EU member states.[86]

---

[78] Priscilla Guo, *No More Safe Harbor*, HARV. POL. REV. (Mar. 20, 2016, 9:57 PM), http://harvardpolitics.com/world/no-more-safe-harbor/ [https://perma.cc/H3VK-CTVD]; *see Schrems*, 2015 E.C.R. ¶¶ 93–94.

[79] *See* McLaughlin, *supra* note 18. *But see* PETER SWIRE, US SURVEILLANCE LAW, SAFE HARBOR, AND REFORMS SINCE 2013, at 10–11 (2015), http://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf [https://perma.cc/LZ9X-47J7] (arguing that NSA programs operate with judicial supervision and only examine the communications of targeted individuals for enumerated foreign intelligence purposes).

[80] *See Schrems*, 2015 E.C.R. ¶¶ 90, 94; Kuner, *supra* note 69, at 242–43; Memorandum from Geoffrey Robertson, *supra* note 48, ¶ 19.

[81] *Schrems*, 2015 E.C.R. ¶ 94; Charter of Fundamental Rights of the European Union, *supra* note 30, art. 7.

[82] *See Schrems*, 2015 E.C.R. ¶ 73; Kuner, *supra* note 46, at 10.

[83] Kuner, *supra* note 46, at 10, 21; Memorandum from Geoffrey Robertson, *supra* note 48, ¶ 19; *see Schrems*, 2015 E.C.R. ¶ 73.

[84] *See Schrems*, 2015 E.C.R. ¶ 94; BOURGEOIS ET AL., *supra* note 63, at 42–43 (quoting EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU 17 (2015)) (defining mass surveillance measures as starting "without prior suspicion or a specific target, which is defined after collection and filtration of certain data"); Kuner, *supra* note 46, at 21; Memorandum from Geoffrey Robertson, *supra* note 48, ¶ 19.

[85] *See Schrems*, 2015 E.C.R. ¶ 94; Bradford, *supra* note 54, at 17–18; Kuner, *supra* note 46, at 10–11; Memorandum from Geoffrey Robertson, *supra* note 48, ¶ 19.

[86] *See* BOURGEOIS ET AL., *supra* note 63, at 43–45; Jens-Henrik Jeppesen, *CJEU General Advocate Opinion in* Schrems *Case a Wake-Up Call*, CTR. FOR DEMOCRACY & TECH. (Sept. 24, 2015),

In requiring third countries to forego all mass surveillance practices in order to participate in legitimate data transfers with the EU, the ECJ effectively tips the global balance in favor of privacy over national security.[87] However, privacy is both a broad and culturally dependent idea and countries around the world balance privacy and national security in different ways.[88] For example, the United States has allowed mass surveillance to occur, despite its detrimental effect on citizens' privacy, due to its efficiency and importance to counterterrorism efforts.[89] Following *Schrems*, however, third countries that engage in data transfers with the EU are barred from making an individualized cost-benefit analysis of utilizing mass surveillance.[90]

The ECJ was an improper forum to sanction the United States for employing mass surveillance practices.[91] In fact, the U.S. government was not even an original party in *Schrems* and, consequently, is not directly bound by the decision.[92] Instead, the *Schrems* decision more directly affected U.S. companies relying on Safe Harbor, prohibiting them from allowing their data transfers with the EU to operate as a medium for government intelligence gathering.[93] However, even if the EU suspended data transfers to U.S. companies, the NSA has the technological capabilities to collect the data directly.[94] To be effective, the prohi-

---

https://cdt.org/blog/cjeu-general-advocate-opinion-in-schrems-case-a-wake-up-call/ [https://perma.cc/B6LR-VQ62]. Snowden revealed that European intelligence agencies operate programs that resemble the NSA's programs and often cooperate with the NSA. Jeppesen, *supra.* In fact, EU member states such as France and the Netherlands have been expanding their ability to execute indiscriminate, mass surveillance practices. Jeppesen, *supra.*

[87] *See Schrems*, 2015 E.C.R. ¶ 94; Bradford, *supra* note 54, at 17–18; Kuner, *supra* note 46, at 10–11; Memorandum from Geoffrey Robertson, *supra* note 48, ¶ 19.

[88] Scott J. Schackelford, *Seeking a Safe Harbor in a Widening Sea*, HUFFINGTON POST: BLOG (Nov. 5, 2015, 12:32 PM), http://www.huffingtonpost.com/scott-j-shackelford/seeking-a-safe-harbor-in-_b_8475670.html [https://perma.cc/V838-WUF6].

[89] *See* Peter Nicholas & Siobhan Gorman, *Obama Defends Surveillance: In Rare Acknowledgement of Antiterror Tactics, President Cites 'Modest Encroachments' in Name of Security*, WALL ST. J. (June 8, 2013), http://www.wsj.com/articles/SB10001424127887324299104578531742264893564 [https://perma.cc/5W7L-DQXK].

[90] *See Schrems*, 2015 E.C.R. ¶ 94; Bradford, *supra* note 54, at 17–18; Kuner, *supra* note 46, at 10–11; Memorandum from Geoffrey Robertson, *supra* note 48, ¶ 19.

[91] *See Schrems*, 2015 E.C.R. ¶ 94; Joel R. Reidenberg, *The Transparent Citizen*, 47 LOY. U. CHI. L.J. 437, 462 (2015).

[92] *See* Mary Carolan & Ciara O'Brien, *High Court Approves US Bid to Join Data Privacy Case*, IRISH TIMES (July 19, 2016, 11:44 AM), http://www.irishtimes.com/business/technology/high-court-approves-us-bid-to-join-data-privacy-case-1.2727075 [https://perma.cc/V78L-RANT]. The U.S. government filed an application to join as an amicus party, meaning it would assist the court on the issue. *Id.* The court granted the U.S. government's application because it had a "legitimate and bona fide interest" in the result of the case. *Id.*

[93] *See Schrems*, 2015 E.C.R. ¶ 94; Daniel Solove, *Sunken Safe Harbor: 5 Implications of* Schrems *and US-EU Data Transfer*, TEACHPRIVACY (Oct. 13, 2015), https://www.teachprivacy.com/sunken-safe-harbor-5-implications-of-schrems-and-us-eu-data-transfer/ [https://perma.cc/F464-SK8N].

[94] *See* Timothy Edgar, Schrems v. Data Protection Commissioner*: Some Inconvenient Truths the European Court of Justice Ignores*, LAWFARE (Oct. 6, 2015, 8:08 PM), https://www.lawfareblog.com/

bition on indiscriminate mass surveillance would likely need to be in the form of an international treaty.[95]

C. Future Compromises

With Privacy Shield in place, the United States has promised to respect the EU's desire for a high level of data protection.[96] The United States, however, is unlikely to honor that promise.[97] The ECJ may decide to respond, like in *Schrems*, by invalidating Privacy Shield and, once again, threatening to suspend data transfers to the United States as leverage to renegotiate for increased data protection standards.[98] In reality, however, the EU is far too economically dependent upon the United States to seriously consider suspending data transfers.[99] In the continued absence of a comprehensive treaty, the EU will therefore have to be willing to recognize that its standards cannot be implemented on a global scale.[100]

Conclusion

In *Schrems,* the ECJ improperly interpreted the DPD and asserted extraterritorial jurisdiction over third countries, but was nevertheless successful in pushing the United States to adopt more robust data protection standards under Privacy Shield. It remains unclear, though, whether Privacy Shield will produce real, tangible change. Going forward, the EU must recognize that data protection standards vary with cultural norms and will likely have no choice but to ignore breaches of Privacy Shield for the sake of economic stability. The EU's unwavering efforts toward implementing its data privacy laws on an international scale only highlight the extent to which technological advances have obscured geographical boundaries. Accordingly, more attention should be given to negotiating an international data protection treaty.

---

schrems-v-data-protection-commissioner-some-inconvenient-truths-european-court-justice-ignores [https://perma.cc/QF8E-957E].

[95] *See* Reidenberg, *supra* note 91.

[96] *See* WEISS & ARCHICK, *supra* note 1, at 12; Kuner, *supra* note 46, at 20.

[97] *See* Kuner, *supra* note 46, at 20–23.

[98] *See id.* at 19–20; WEISS & ARCHICK, *supra* note 1, at 12.

[99] *See* WEISS & ARCHICK, *supra* note 1, at 8 (discussing the European Commission's three broad priorities for ensuring that EU-U.S. data transfers occur while Safe Harbor is re-negotiated).

[100] *See* Reidenberg, *supra* note 91.