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

Follow this and additional works at: http://lawdigitalcommons.bc.edu/iclr

Part of the Administrative Law Commons, Comparative and Foreign Law Commons, Computer Law Commons, Courts Commons, European Law Commons, International Law Commons, Internet Law Commons, Jurisdiction Commons, National Security Law Commons, Privacy Law Commons, and the Transnational Law Commons

Recommended Citation

This Comments is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College International and Comparative Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact nick.szydlowski@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.


fers between the EU and the United States. 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). 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. 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. 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.

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. 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.
5 See WEISS & ARCHICK, supra note 1, at 8–9.
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.”

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.

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. 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. 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.

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.” 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. Shortly thereafter, the Commission recognized the Safe Harbor Privacy Principles as ensuring an adequate level of data protection in its Safe Harbor Decision. 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

---


11 Id. art. 25.


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.  

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. 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. 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. The Commissioner further held that Schrems lacked evidence that the NSA had, in fact, accessed his personal data. 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.

II. DISCUSSION  

A. Questions Before the Court  

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

---


19 Id. ¶¶ 30, 36.


22 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. 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. Beyond the Irish High Court’s two questions, the ECJ also considered the broader issue of whether Safe Harbor was consistent with EU law.

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). 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. Article 28 of the DPD requires member states to set up at least one public authority to monitor compliance. Articles 7, 8, and 47 of the EU Charter protect individual rights to privacy, data protection, and an effective remedy and fair trial, respectively.

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

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. 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.” Although the ECJ recognized that DPAs have a significant amount of authority, only the court has the authority to invalidate Commission decisions.

After identifying the court and Commissioner’s authority, the ECJ assessed Safe Harbor, ultimately finding it invalid. 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.” 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.

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


33 See Pfeifle, supra note 31.
34 Id.
35 Id.
37 Id. ¶ 99.
38 See id. ¶ 62.
39 Id. ¶¶ 100–103, 106.
40 Id. ¶ 73 (emphasis added).
41 Id. ¶¶ 73, 86–87.
judicial remedy. 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. 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. However, the Commission did not evaluate U.S. laws and international commitments when issuing Safe Harbor.

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. On February 2, 2016, an agreement was officially reached on “Privacy Shield” and the Commission issued its adequacy finding on July 12, 2016. 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. Even with Privacy Shield in effect, it is unlikely that the EU will see the desired reforms in U.S. intelligence practices.

---

42 Id. ¶¶ 81, 89, 95.
43 Id. ¶¶ 81, 89.
44 Id. ¶ 83.
45 Id.
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”

52 Id. ¶ 73; see Kuner, supra note 46, at 17.
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.
58 See Schrems, 2015 E.C.R. ¶ 73; Equivalent, supra note 55; Essentially, supra note 57.
which is “appropriate.” Even under the more generous French definition, “adequate” seems to imply a lesser standard than “essentially equivalent.” 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.”

The essentially equivalent standard is not only contrary to the DPD’s plain language, but also to its overall structure. 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. 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. The essentially equivalent standard, however, significantly reduces the Commission’s discretion to issue findings of adequacy. 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.

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.
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; BOURGEOS ET AL., supra note 63.
66 See Schrems, 2015 E.C.R. ¶ 73; VARJU, supra note 63; BOURGEOS ET AL., supra note 63, at 27.
67 See Schrems, 2015 E.C.R. ¶ 73; BOURGEOS 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

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.
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. Admittedly, U.S. law and practice allow for large-scale data collection. 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.

The court found U.S. mass surveillance practices to be inconsistent with the right to private life under Article 7 of the EU Charter. 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.” The DPD therefore extraterritorially binds third countries to the EU Charter and places a “per se limit” on mass surveillance practices. 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. 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. 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.

---

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.
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; BOURGOIS 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 BOURGOIS 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. However, privacy is both a broad and culturally dependent idea and countries around the world balance privacy and national security in different ways. 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. 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.

The ECJ was an improper forum to sanction the United States for employing mass surveillance practices. In fact, the U.S. government was not even an original party in *Schrems* and, consequently, is not directly bound by the decision. 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. However, even if the EU suspended data transfers to U.S. companies, the NSA has the technological capabilities to collect the data directly. To be effective, the prohi-
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.