GLOBAL DATA PRIVACY: THE EU WAY

PAUL M. SCHWARTZ*

EU data protection law is playing an increasingly prominent role in today's global technological environment. The cornerstone of EU law in this area, the General Data Protection Regulation (GDPR), is now widely regarded as a privacy law not just for the EU, but for the world. In the conventional wisdom, the EU has become the world's privacy cop, acting in a unilateral fashion and exercising de facto influence over other nations through its market power. Yet, understanding the forces for convergence and divergence in data privacy law demands a more nuanced account of today's regulatory environment.

In contrast to the established narrative about EU power, this Article develops a new account of the diffusion of EU data protection law. It does so through case studies of Japan and the United States that focus on how these countries have negotiated the terms for international data transfers from the EU. The resulting account reveals the EU to be both collaborative and innovative.

Three important lessons follow from the case studies. First, rather than exercising unilateral power, the EU has engaged in bilateral negotiations and accommodated varied paths for non-EU nations to meet the GDPR's "adequacy" requirement for international data transfers. Second, while the adequacy requirement did provide significant leverage in these negotiations, it has been flexibly applied throughout its history. Third, the EU's impressive regulatory capacity rests on a complex interplay of institutions beyond the European Commission. Not only are there a multiplicity of policy and lawmaking institutions within the EU, but the EU has also drawn on non-EU privacy innovations and involved institutions from non-EU countries in its privacy policymaking.

Finally, this Article identifies two overarching factors that have promoted the global diffusion of EU data protection law. The first such factor regards legal substance. Public discourse on consumer privacy has evolved dramatically, and important institutions and prominent individuals in many non-EU jurisdictions now acknowledge the appeal of EU-style data protection. Beyond substance, the EU has benefited from the accessibility of its omnibus legislative approach; other jurisdictions have been drawn to the EU's highly transplantable legal model. In short, the world has weighed in, and the EU is being rewarded for its success in the marketplace of regulatory ideas.

 For their helpful comments on this paper, I wish to thank Eremipagamo M. Amabebe, Michelle Gal, Brittany Johnson, Margot Kaminski, Annie Lee, and Amelie Raepple.

INTRODUCTION

On May 25, 2018, the General Data Protection Regulation (GDPR) took effect throughout the European Union.[1] A swell of voices worldwide greeted this watershed occasion, which we can term "GDPR Day." Amid the memes and clamor over the GDPR's high sanctions, many commenters noted that it represented a law not only for the EU, but for the world.[2] The EU had become the world's privacy cop. It was said to have "opened a new chapter in the history of the Internet," and to have acted to protect a fundamental human right to privacy.[3] Indeed, even while criticizing the GDPR for its vagueness and on other grounds, U.S. Secretary of Commerce Wilbur Ross essentially conceded its stature by noting that

1 *See* Quentin Ariès et al., *As Europe's Data Law Takes Effect, Watchdogs Go After Tech Companies*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/world/as-europes-data-law-takes-effect-watchdogs-go-after-tech-companies/2018/05/25/25b66320-79a0-493d-b62a-a136698cc1a3_story.html (describing the effects of the "sweeping" data-protection law in Europe).

2 *See e.g.*, Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html; Sarah Gordon & Aliya Ram, *Information Wars: How Europe Became the World's Data Police*, FIN. TIMES (May 20, 2018), https://www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8.

3 Helen Dixon, *Regulate to Liberate: Can Europe Save the Internet?*, FOREIGN AFF., Sept.–Oct. 2018, https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate ("In a world increasingly defined by digital technology, the protection of private data is not merely a luxury; it is a 'fundamental right,' as the text of the GDPR notes.").

companies in the United States "have already invested billions of dollars to comply with the new rules" it creates.[4]

Proof of the influence of the GDPR and EU data protection law, however, goes beyond the hefty sums spent by U.S. companies to comply with them. The EU has taken an essential role in shaping how the world thinks about data privacy. Even corporate America draws on EU-centric language in discussing data privacy. Two examples will suffice to demonstrate this cultural shift. Four days before GDPR Day, Brad Smith, the President of Microsoft, tweeted, "We believe privacy is a fundamental human right."[5] In a similar fashion, Tim Cook, the CEO of Apple, told CNN that "privacy is a fundamental human right."[6] The description of privacy through rights discourse is a core aspect of the EU approach to data privacy. Data protection in the EU is seen as a fundamental right, and one that rests on interests in dignity, personality, and informational self-determination.[7] In contrast, the U.S. legal system views information privacy as based largely on a consumer interest.[8] It situates individuals in a data marketplace in which they are to be free to engage in data exchanges, and the law is to police data trades for unfairness, deceptions, and other market failures.[9]

The question then becomes *why* the world follows the EU's lead in this area. Data privacy is one of the most important areas of law in today's global digital economy, so understanding its diffusion is of critical importance. Answering this question, however, requires a sense of *how* the world has followed the EU in this area. This Article will argue that, contrary to the one-fell-swoop perception of EU influence evoked by GDPR Day, there has, in fact, been a varied range of nation-state, transnational, and corporate behavior that has helped spread EU data protection throughout the world.

Part I of this Article first discusses the reception of the GDPR as a milestone in data law. It then examines prior academic work regarding the transmission of the EU model of data privacy. Both Jack Goldsmith and Tim Wu, as well as Anu Bradford, have depicted the EU's influence as a

---

4 Wilbur Ross, *EU Data Privacy Laws Are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c.

5 Brad Smith (@BradSmi), TWITTER (May 21, 2018, 1:40 PM), https://twitter.com/BradSmi/status/998664978063241216.

6 *Apple CEO: Privacy Is Fundamental Human Right*, CNN (June 5, 2018), https://www.cnn.com/videos/cnnmoney/2018/06/05/tim-cook-apple-ceo-privacy-human-right-intv-segall.cnn (video interview with Laurie Segall).

7 Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 123–27 (2017).

8 *Id.* at 132–37.

9 *Id.* at 136–37.

kind of unilateral power.[10] In particular, Bradford's model portrays a powerful "Brussels Effect" that largely rests on the EU's "de facto unilateral" influence.[11] This Article ultimately presents and advocates for a different account of the EU's influence on global data privacy.

Part II presents two case studies of the global diffusion of EU data protection law. It begins by analyzing the EU's adequacy requirement for international transfers of personal data from the EU. As a long-standing matter of EU jurisprudence, international data transfers are permitted to "third countries"—that is, non-EU countries—only if they have "adequate" protections in place for this information.[12] Armed with a concomitant data embargo power, the EU has engaged in separate adequacy negotiations with Japan, the United States, and other countries.[13] In Japan, these negotiations have taken the form of an application for a determination of adequacy from the European Commission.[14] The United States, on the other hand, has worked closely with the EU to craft two successive agreements that permit private companies to voluntarily follow EU privacy standards.[15]

Part III draws lessons from these case studies. First, this Part finds that the EU has demonstrated considerable negotiating flexibility. The case studies show openness to varied and customized approaches, rather than rigid exercises of unilateral de facto power. Second, the EU's adequacy requirement has provided the EU with important negotiating leverage. The EU has exercised this leverage within a policy environment that contains multiple factors working to promote the diffusion of EU privacy law. Third, the case studies demonstrate that the EU's regulatory capacity arises from a complex interplay among EU institutions and outside influences—not simply through "Brussels" exercising power as a monolithic entity. For instance, the European Court of Justice has assumed an important role in this area by anchoring EU data protection in the European Charter of Fundamental Rights, thereby constitutionalizing EU data protection law.[16]

This Part ends by pointing to two overarching factors that have promoted the global diffusion of EU data protection. As an initial factor, legal substance has been important. Beyond the force of EU market power and its negotiating prowess, the widespread influence of EU data protection reflects a success in the marketplace of regulatory ideas.[17] As a second

10 *See infra* Section I.B.
11 *See infra* notes 47–79 and accompanying text.
12 *See infra* Section II.A.
13 *See infra* Section II.B.
14 *See infra* Section II.B.1.
15 *See infra* Section II.B.2.
16 *See infra* Section II.B.2.ii.
17 *See infra* Section II.B.2.ii.

factor, the EU has benefited from its use of a highly accessible legal model. It has relied on omnibus regulations that cover both private and public sectors, and have thus proved easy for other nations to adopt.[18] But this model was not developed with international ambitions in mind. Rather, the EU turned to an omnibus legislative approach in response to an internal issue that it faced in the 1970s: how to harmonize the data processing practices of its member states.[19]

Finally, a few words about terminology. For conceptual clarity, this Article employs three related but distinct terms: "data protection," "information privacy," and "data privacy." "Data protection" is the accepted, standard term applied to Europe's body of law concerning the processing, collection, and transfer of personal data. Although U.S. law lacks such a universally accepted term, it generally relies on the expression "information privacy."[20] When this Article discusses the concept in neutral terms, it uses "data privacy" or "privacy." For example, "data privacy" may refer to this area generally, or to the emerging body of transnational law that is based on inputs from many countries.

I
DATA PRIVACY: THE EU WAY

Media coverage of GDPR Day demonstrates general agreement about the widespread influence of EU data protection law. This Part first describes this consensus and then considers the leading explanations for the EU's influence in this area. It draws first from Goldsmith and Wu's scholarship and then from Bradford's model, which characterizes the EU as wielding de facto unilateral power.

A. Happy GDPR Day

Extensive media coverage, conferences, speeches, and the tweeting of memes marked GDPR Day.[21] The numerous memes devoted to the GDPR drew on popular culture, including the character Jules Winnfield from *Pulp*

18 *See infra* Section II.B.2.ii.

19 *See infra* Section III.B.

20 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1094–96 (6th ed. 2018) (introducing thematic differences between privacy law in the United States and the EU); *see also, e.g.*, *The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the Subcomm. on Commerce, Trade & Consumer Prot. of the H. Comm. on Energy & Commerce*, 107th Cong. 68 (2001) [hereinafter Reidenberg Statement] (statement of Joel R. Reidenberg, Professor of Law, Fordham University School of Law) ("[T]he United States has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights. . . . In this context, European democracies approach *data protection* as an element of public law." (emphasis added)).

21 *See* Angela Watercutter, *How Europe's GDPR Regulations Became a Meme*, WIRED (May 25, 2018, 12:16 PM), https://www.wired.com/story/gdpr-memes.

Fiction[22] brandishing a gun with the caption, "Say GDPR One More Time!!!"[23] and a parody of the initial screen crawl from *Star Wars*[24] ("We have updated our GLOBAL PRIVACY TERMS. Your trust is important to us," followed by additional, likely endless, boilerplate).[25] TrustArc, a leading vendor in privacy compliance technology, even handed out "GDPR Recovery" kits—small nylon zipper bags containing Ibuprofen, vitamin C, and similar hangover remedies—at industry conferences.[26] Finally, in the period immediately before GDPR Day, search interest in the term "GDPR" exceeded that for either "Beyoncé" or "Kim Kardashian."[27]

Substantively, observers of GDPR Day emphasized the high sanctions and aggressive enforcement available under the regulation.[28] For example, the GDPR permits fines up to 4% of a company's worldwide revenue or 20 million Euros, whichever is greater.[29] The GDPR also creates a new class-action-like remedy in data protection law: Article 80 grants individuals "the right to mandate a not-for-profit body, organization or association . . . to lodge [a] complaint on his or her behalf."[30] This provision empowers non-governmental organizations (NGOs) to assist in enforcement. On GDPR Day, the *Washington Post* reported that privacy groups had wasted no time in using this provision to allege that tech giants such as Amazon, Facebook, and Google were "mishandling consumers' personal data."[31] These NGOs

---

22 *Pulp Fiction (1994) - Samuel L. Jackson: Jules Winnfield*, IMDB, https://www.imdb.com/title/tt0110912/characters/nm0000168 (last visited Mar. 28, 2019).

23 Cardens Accountants (@CountOnCardens), TWITTER (May 18, 2018, 10:37 AM), https://twitter.com/CountOnCardens/status/997410776389439489.

24 *Star Wars: Episode IV – A New Hope – Opening Crawl*, STAR WARS, https://www.starwars.com/video/star-wars-episode-iv-a-new-hope-opening-crawl (last visited Mar. 28, 2019).

25 Rian Johnson (@rianjohnson), TWITTER (May 24, 2018, 12:15 PM), https://twitter.com/rianjohnson/status/999730569641525248.

26 *See* Dr. Tobias Graeber (@ThinkPrivate), TWITTER (Apr. 3, 2018, 1:27 AM), https://twitter.com/ThinkPrivate/status/981085739369881600; *see also* PRNewswire, *TrustArc Expands Industry Leading Compliance Solutions with First Privacy Certification for Data Processors*, MARTECH SERIES (Sept. 11, 2018, 5:40 PM), https://martechseries.com/analytics/data-management-platforms/privacy-and-regulations/trustarc-expands-industry-leading-compliance-solutions-first-privacy-certification-data-processors (describing TrustArc as "the leading data privacy management company").

27 *GDPR in Numbers*, EUR. COMMISSION (Jan. 25, 2019), https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf.

28 *See, e.g.*, Neil Hodge, *Don't Expect Grace Period for GDPR Enforcement*, COMPLIANCE WK. (Apr. 24, 2018), https://www.complianceweek.com/news/news-article/dont-expect-grace-period-for-gdpr-enforcement.

29 *See* Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 83(5), 2016 O.J. (L 119) 1 [hereinafter GDPR].

30 *Id.* art. 80(1).

31 Ariès et al., *supra* note 1.

were said to be placing tech companies under "new legal siege."[32] Striking a similar tone, the *New York Times* quoted Irish Data Protection Commissioner Helen Dixon's message to tech companies that she intends "to use her new powers 'to the fullest.'"[33]

Moreover, there is agreement in the academic literature about the pathbreaking impact of EU privacy law. In a co-authored treatise, Jan Albrecht called the GDPR "without any doubt the most important legal source for data protection."[34] Albrecht is in a good position to comment on the GDPR; he served as a key figure in its creation as the Parliament's rapporteur for the law.[35] Additionally, in a census of global data privacy laws, Australian law professor Graham Greenleaf found that 120 countries have now enacted EU-style data privacy laws.[36] Greenleaf noted that at least thirty more countries had official bills for such laws.[37] In his assessment, "[S]omething reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws."[38]

Furthermore, principles found in the GDPR, such as "data portability" and the "right to be forgotten," are already influencing laws outside Europe.[39] In a 2018 speech in Brussels, Greenleaf observed of these two concepts, "There is already a surprisingly high amount of enactment of such principles outside Europe, influenced by the GDPR's development since 2011."[40] This allusion to 2011 rightly serves as a reminder of the GDPR's long period of gestation. The law took effect in May 2018 after a two-year grace period for compliance, but plans for its enactment and

---

32 *Id.*

33 Adam Satariano, *New Privacy Rules Could Make This Woman One of Tech's Most Important Regulators*, N.Y. TIMES (May 16, 2018), https://www.nytimes.com/2018/05/16/technology/gdpr-helen-dixon.html.

34 JAN PHILIPP ALBRECHT & FLORIAN JOTZO, DAS NEUE DATENSCHUTZRECHT DER EU 7 (2017) (author's translation).

35 Martin Banks, *Business Groups Call for Leniency Ahead of GDPR Entry into Force*, PARLIAMENT MAG. (May 18, 2018), https://www.theparliamentmagazine.eu/articles/news/business-groups-call-leniency-ahead-gdpr-entry-force.

36 *See* Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, PRIVACY LAWS & BUS. INT'L REP., Feb. 2017, at 10, 10–13.

37 *See id.* at 10.

38 Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 77 (2011).

39 *Id.* at 79; *see* GDPR, *supra* note 29, arts. 17, 20.

40 Graham Greenleaf, *Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018*, at 3 (Univ. of N.S.W. Law, Research Paper No. 18–56, 2018), https://ssrn.com/abstract=3184548.

debates about its content had begun long before.[41] As a result, the ideas found in the GDPR have percolated and spread globally for close to a decade.

B. Theories of Data Privacy Diffusion

A variety of legal disciplines have examined the questions of how and why legal principles and norms spread between jurisdictions. This Article first examines the influential work of Jack Goldsmith and Tim Wu regarding the worldwide diffusion of EU privacy law. It then turns to the valuable scholarship of Anu Bradford, which comes to similar conclusions about the EU's singular power.

Goldsmith and Wu argue that the EU has become the effective sovereign in this area because it employs a "[u]nilateral global [privacy] law" that "results from the unusual combination of Europe's enormous market power and its unusual concern for its citizens' privacy."[42] Because the EU is a highly important marketplace for international companies, many companies do not have the option of "pull[ing] out of the European market altogether."[43] Furthermore, under many circumstances, international companies cannot geographically screen their EU customers and, even if they could, would not wish to create separate services for them.[44] Finally, because the EU cares greatly about privacy and has been long involved in legislating rules in this area, its regulations have extraterritorial reach: Its laws follow the personal data of EU residents whenever and wherever the information is transferred outside the EU.[45] The result, according to Goldsmith and Wu, is that U.S. companies have chosen to bow to the "significant market power" of the EU.[46]

Bradford has further developed this idea of unilateral EU lawmaking. In her article *The Brussels Effect*, Bradford, like Goldsmith and Wu, seeks to explain the EU's seeming ability to impose its rules on a global basis.[47] Beyond privacy, Bradford examines a number of areas, including antitrust, consumer protection, and environmental protection.[48] As she points out, EU

41 *See The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Feb. 9, 2019).

42 JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 176 (2006).

43 *Id.* at 175.

44 *See, e.g.*, *id.* at 174–76 (discussing Microsoft's decision to implement major changes to its dot-NET Passport system worldwide instead of just in Europe).

45 *See id.* at 176 ("Europe cares more about privacy than other regions and therefore sets the standard for privacy.").

46 *Id.*

47 *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

48 *Id.* at 19–35.

regulations have "a tangible impact on the everyday lives of citizens across the world."[49] By way of concrete examples, Bradford writes, "Few Americans are aware that EU regulations determine the makeup they apply in the morning, the cereal they eat for breakfast, the software they use on their computer, and the privacy settings they adjust on their Facebook page. And that's just before 8:30 AM."[50] Here is proof of the "Brussels Effect."[51]

Expanding Goldsmith and Wu's identification of unilateral power in EU privacy law, Bradford further specifies that the Brussels Effect is one of de facto "unilateral regulatory globalization."[52] This situation occurs "when a single state is able to externalize its laws and regulations outside of its borders through market mechanisms, resulting in the globalization of standards."[53] The global rule of the EU is generally not based on law (de jure) because states outside of the EU remain formally bound only by their domestic laws. Yet, private parties in these countries increasingly follow EU law.[54] As Bradford writes, "While the EU regulates only its internal market, multinational corporations often have an incentive to standardize their production globally and adhere to a single rule."[55]

Sometimes, through a two-step process, law can play a formal role as well. According to Bradford, after export-oriented firms have adjusted their business practices to follow the EU's standards, they sometimes lobby their own governments to enact the same standards in order to gain a competitive advantage in their home nation against their non-export-oriented counterparts.[56] Here, there would be a "de jure Brussels Effect," which Bradford conceives of as following a set timeline.[57] As Bradford writes, "Corporations' de facto adjustment to the EU rules paves the way for legislators' de jure implementation of these rules . . . ."[58]

Bradford also identifies a number of factors that will promote a Brussels Effect in a given area. The critical factors begin with the presence of "a large domestic market, significant regulatory capacity, and the propensity to enforce strict rules over inelastic targets (e.g. consumer markets) as opposed to elastic targets (e.g. capital)."[59] A final factor

49 *Id.* at 3.
50 *Id.*
51 *Id.*
52 *Id.* at 5.
53 *Id.* at 3.
54 *Id.* at 8 ("We typically see only a 'de facto regulatory convergence' whereby much of global business is conducted under unilateral EU rules even when other states continue to maintain their own rules.").
55 *Id.* at 6.
56 *Id.*
57 *See id.* at 8.
58 *Id.*
59 *Id.* at 5.

concerns whether a firm's conduct or production is "nondivisible," meaning that it would not be feasible to have different standards for different markets.[60] As Bradford explains, a firm's inability to set up different compliance standards—whether for legal, technical, or economic reasons—creates a powerful condition enabling "a jurisdiction to dictate rules for global commerce."[61]

Under Bradford's factors, there is indeed much evidence that suggests a de facto unilateral Brussels Effect for privacy. First, the EU is a rich consumer market, and an important one for large corporations outside of it. Goldsmith and Wu rightly emphasize this point.[62] The EU represents the second largest economy in the world, and the second largest consumer market in the world.[63] More specifically, consumers in the EU have been early adopters of a wide range of information technology, and the EU has been a leader in critical areas such as broadband internet service.[64] International tech giants have moved quickly to offer their products and services in the EU,[65] which has been an important source for these entities' gathering of personal data. As just one example, Facebook has more users in Europe (17.3% of its world users) than in North America (13.3%).[66]

---

60 *Id.*

61 *Id.*

62 GOLDSMITH & WU, *supra* note 42, at 175 (discussing the strength of Europe's consumer market and how that impacted Microsoft in the early 2000s).

63 In 2017, China led the world with a GDP of $23.21 trillion, followed by the EU ($20.85 trillion) and the United States ($19.49 trillion). *The World Factbook*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook (locate dropdown menu marked "Please select a country to view"; select "China," "European Union," or "United States"; scroll down and expand "Economy" subsection) (last visited Feb. 9, 2019). The size of the economy was taken from GDP (purchasing power parity), and the consumer market was determined by multiplying the population with the GDP per capita. *Id.*

64 In 2010, the European Commission launched the Europe 2020 Strategy, which included as one of its flagship initiatives a Digital Agenda for Europe (DAE). The DAE set a goal for a Digital Single Market where "[a]ll Europeans should have access to high speed internet by 2013." European Commission Press Release IP/10/225, Europe 2020: Commission Proposes New Economic Strategy in Europe (Mar. 3, 2010). The DAE also "proposes to better exploit the potential of Information and Communication Technologies (ICTs) in order to foster innovation, economic growth and progress." *Europe 2020 Strategy*, EUR. COMMISSION, https://ec.europa.eu/digital-single-market/en/europe-2020-strategy; *see also* European Commission Press Release IP/13/968, 100% Basic Broadband Coverage Achieved Across Europe—EU Target Achieved Ahead of Schedule. Next Stop Is Fast Broadband for All. (Oct. 17, 2013) (stating that European satellite companies Eutelstat and Astra are "world leaders in satellite broadband" and that 148 of the 250 active broadband satellites at the time were European-operated).

65 *See, e.g.*, Matthew Hughes, *Europe Isn't the Next Silicon Valley. It's Better*, NEXT WEB (May 22, 2017), https://thenextweb.com/eu/2017/05/22/europe-isnt-the-new-silicon-valley-its-better (explaining how technology companies are expanding rapidly into Europe).

66 *Facebook Users in the World*, INTERNET WORLD STATS, https://www.internetworldstats.com/facebook.htm (last visited Mar. 31, 2019) (listing Facebook subscriber information as of June 30, 2017).

Second, the EU has built up considerable regulatory capacity for privacy. At the member state level, each country has a Data Protection Authority (DPA).[67] DPAs are a long-established feature of EU data protection.[68] The GDPR lists the required tasks of these officials, which include assisting individuals in protecting their rights, advising legislatures on the functioning of existing regulation, and enforcing the law.[69] Within the EU, data protection has long been a focus of Directorates-General (DGs).[70] DGs are part of the European Commission (Commission), the executive arm of the EU, and each is devoted to a specific field or fields of expertise.[71] The Parliament also demonstrates strong interest in this topic, with the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) currently playing a central role.[72] Finally, there are important independent EU privacy entities, including the European Data Protection Supervisor[73] and, under the GDPR, the European Data Protection Board.[74] There are sometimes distinct, sometimes collaborative, sometimes overlapping roles for these bodies, which has led to a complex and rich policy environment for developing data protection.

---

67 *See National Data Protection Authorities*, EUR. COMMISSION, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080 (last visited Mar. 31, 2019) (listing the current members of the European Data Protection Board from each country in the EU).

68 *How Did We Get Here?*, EUGDPR.ORG, https://eugdpr.org/the-process/how-did-we-get-here (last visited Aug. 4, 2019) (explaining that DPAs were first established in EU member states in 1995).

69 GDPR, *supra* note 29, art. 57. In the judgment of Kerstin Kreul, the GDPR "significantly expands the range of responsibilities of the Data Protection Authorities." Kerstin Kreul, Artikel 57, *in* SIBYLLE GIERSCHMANN ET AL., KOMMENTAR DATENSCHUTZ-GRUNDVERORDNUNG 1173 (2018) (author's translation).

70 For example, the then Directorate General XV commissioned a 1998 report from Joel Reidenberg and me on the privacy implications of emerging online services. *See* JOEL R. REIDENBERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES (1998), https://paulschwartz.net/wp-content/uploads/2019/01/onlinesvcs_schwartz-reidenberg.pdf. Two years earlier, the Directorate General XIII had commissioned a report from us on the overall status and contours of U.S. information privacy. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996).

71 *See How the Commission Is Organised*, EUR. COMMISSION, https://ec.europa.eu/info/about-european-commission/organisational-structure/how-commission-organised_en (last visited Mar. 31, 2019).

72 The LIBE Committee "has played a key role in developing the [GDPR]" as well as in "investigating the Facebook Cambridge-Analytica breach[,] updating the ePrivacy Regulation, . . . [and] reviewing the EU-U.S. Privacy Shield." *LIBE Committeee* [sic], ELECTRONIC PRIVACY INFO. CENT., https://epic.org/privacy/intl/LIBE/default.html (last visited Feb. 9, 2019).

73 The first European Data Protection Supervisor was appointed in 2004. *See* Decision 2004/55/EC, of the European Parliament and of the Council of 22 December 2003 Appointing the Independent Supervisory Body Provided For in Article 286 of the EC Treaty (European Data Protection Supervisor), art. 1, 2004 O.J. (L 12) 47.

74 *See* GDPR, *supra* note 29, art. 68.

Third, regarding a predisposition to enforce strict rules on inelastic markets, Bradford argues that the EU generally favors "precautionary regulatory action . . . even in the absence of an absolute, quantifiable certainty of the risk."[75] As for the elasticity of personal data markets, Bradford finds that companies may face difficulties in isolating services exclusively for EU operations.[76] Here, too, is a point raised by Goldsmith and Wu. Services may no longer "scale" profitably enough for global internet concerns if they are tailored to geographical locations, and there may be political backlash if some non-EU customers feel they are receiving poorer levels of privacy.[77] A contrast should be drawn with labor standards, where companies may be more easily able to isolate employment practices country-by-country.[78] As Bradford observes, labor markets are easily divisible, but data services are not.[79] In her framework, global standards emerge when a company's "production or conduct is nondivisible across different markets or when the benefits of a uniform standard due to scale economies exceed the costs of foregoing lower production costs in less regulated markets."[80] Overall, according to Bradford, personal data appears to fulfill the conditions for a de facto unilateral Brussels Effect.[81]

Testing this hypothesis, the next Part looks at two case studies involving the diffusion of EU data protection worldwide. In the first, Japan engaged in the formal process of seeking an adequacy finding that would allow international data transfers from the EU following adoption of a Japanese law modeled on EU-style data protection.[82] In the second, the United States went outside of the formal adequacy process and negotiated opt-in agreements for U.S. companies that wish to comply with EU standards.[83] Ultimately, this Article finds that Bradford's Brussels Effect does not fully capture the dynamic present in the global negotiations around data privacy. At the same time, Bradford is describing a far wider field of EU influence than privacy, and it may well be that her model fits

75 Bradford, *supra* note 47, at 15.

76 *Id.* at 25 ("'[D]ata flows lightly and instantly across borders.'… At times, it is technologically difficult or impossible to separate data involving European and non-European citizens." (quoting *The Clash of Data Civilisations*, ECONOMIST (June 17, 2010), https://www.economist.com/international/2010/06/17/the-clash-of-data-civilisations)).

77 *See* GOLDSMITH & WU, *supra* note 42, at 175–77.

78 Bradford, *supra* note 47, at 18–19 ("A corporation can maintain different standards in different jurisdictions without difficulty—ranging from working hours and vacation policies to retirement plans and collective labor strategies.").

79 *See id.* at 18 ("Unable to isolate its data collection for the EU for technical reasons, Google is forced to adjust its global operations to the most demanding EU standard.").

80 *Id.* at 17.

81 *See id.* at 22–26 (discussing each of the conditions for the Brussels Effect in the context of privacy regulation).

82 *See infra* Section II.B.1.

83 *See infra* Section II.B.2.

these other areas of law. Her analysis also undeniably greatly advances the scholarship surrounding the global diffusion of EU law.

II
GLOBAL ENGAGEMENT WITH EU DATA PROTECTION

As the preceding Part has shown, a consensus exists regarding the worldwide influence of EU data protection law. This Part examines a foundational element of EU data protection law, namely its adequacy requirement. It then turns to case studies of two countries' attempts to meet this standard. These case studies permit scrutiny of the Brussels Effect.

A. The Adequacy Requirement

As a technological matter, digital data can be transmitted throughout the world in a largely friction-free exercise. Consequently, Europe's efforts since the 1970s to create strong safeguards for individual privacy would be doomed to failure if the reach of its laws ended at the borders of Europe.[84] The danger would be a processing of the personal information of EU citizens in privacy-free data oases. The EU has therefore attached its data protection regime to all personal information from the EU regardless of where it flows, and it has granted EU authorities a "data embargo power" that permits blocking data exports to nations that do not meet EU privacy requirements.[85]

The standard for extraterritorial transmissions of personal data has long been that of "adequacy" of data protection in the foreign jurisdiction.[86] In 1995, the Directive on Data Protection (Directive), the precursor to the GDPR, established an adequacy requirement for international data transmissions.[87] In 2016, the GDPR maintained this same requirement and strengthened the process around it.[88] Under both the Directive and the GDPR, adequacy can be met by a country's law as a whole, by a sub-territory within a country, or by the terms of a specific transfer.[89] Along

84 *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995) [hereinafter Schwartz, *European Data Protection Law*].

85 Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1966, 1984 (2013) [hereinafter Schwartz, *The EU-U.S. Privacy Collision*].

86 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, art. 25, 1995 O.J. (L 281) 31, 45–46 [hereinafter Council Directive 95/46/EC].

87 *Id.*

88 *See* GDPR, *supra* note 29, arts. 44–50, recitals 103–07 (substantially broadening the catalogue of adequacy requirements and increasing their detail).

89 *See id.*; *see also* Julian Wagner, *The Transfer of Personal Data to Third Countries Under*

with the ability to determine adequacy, the EU also created a concomitant ability for its regulators to block transfers wherever they do not find adequacy.[90]

The history of the adequacy requirement reveals that it was the product of a compromise. Prior to the Directive, many EU nations required "equivalent protection" in another country before allowing personal data to be transferred beyond their borders.[91] The Directive took this equivalency standard and limited it to members of the EU.[92] Under the Directive, member states were obliged to enact harmonizing legislation and to permit transfers *inside* the EU without any further formalities.[93] In this fashion, the Directive helped create a single market for personal data in the EU—one constructed at a similarly high level of safeguards. For transfers *outside* the EU, however, the Directive did not look to equivalency, but used a different benchmark, that of adequacy of protection.[94]

The Directive stated that international transfers were to be permitted "only if . . . the third country in question ensures an adequate level of protection."[95] The decision as to adequacy was to be made by regulators at the member state level, although the Commission itself was authorized to "enter into negotiations" with countries with inadequate data protection "with a view to remedying the situation."[96] The Directive also contained six exceptions to its adequacy requirement for international transfers, including one where the "data subject" consented to the transmission.[97] Finally, the Directive called for the Commission to maintain a whitelist of countries with adequate data protection.[98] There are now twelve entities on this list that the EU can transfer data to without any further requirements.[99]

the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?, 8 INT'L DATA PRIVACY L. 318, 320 (2018) ("In the absence of such an adequacy decision, an export is . . . only allowed if additional safeguards are provided, such as [binding corporate rules] and standard data protection clauses adopted by the [European Commission].").

90 *See* Council Directive 95/46/EC, *supra* note 86, art. 25(4) (preventing transfer of data to a third country that does not ensure an adequate level of protection); GDPR, *supra* note 29, art. 44, at 60 (blocking transfer of data unless "the conditions . . . are complied with by the controller and processor").

91 Schwartz, *European Data Protection Law*, *supra* note 84, at 474–77 (summarizing the requirements of several European countries in 1995 and finding an emerging consensus around the equivalency standard).

92 Council Directive 95/46/EC, *supra* note 86, recital 8 (establishing the limited relationship).

93 *Id.* recital 9; Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 85, at 1973–74.

94 *See* Council Directive 95/46/EC, *supra* note 8684, art. 25(1).

95 *Id.*

96 *Id.* art. 25(5).

97 *Id.* art. 26(1).

98 *Id.* art. 30(6).

99 *See Adequacy Decisions*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (last visited Mar. 31, 2019) (listing Andorra, Argentina, Canada, Faroe Island, Guernsey, Israel, Isle of

A transmission to a nation on the whitelist is the functional equivalent of a transfer within the EU.

In contrast to a directive, a regulation such as the GDPR supplies directly binding law to the member states.[100] Similarly to the Directive, the GDPR provides an adequacy test for transfers of data outside of the EU. In its Article 45, the GDPR requires that the Commission consider a long list of factors in assessing the adequacy of protection, including "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral . . . as well as the implementation of such legislation, data protection rules, professional rules and security measures."[101]

The EU's internal procedures for finding adequacy have changed over the years.[102] Today, a finding of adequacy involves a formal proposal from the Commission; an opinion of the European Data Protection Board, which consists of representatives from each member state's data protection authorities; an approval from member state representatives through the so-called "comitology" procedure; and the adoption of the adequacy decision by the European Commissioners.[103]

Here is a source of power for the EU that might appear to encourage de facto unilateralism à la Bradford. With the authority to prohibit data flows, the EU clearly does have leverage regarding the terms for data processing in non-EU nations. The next Section examines the EU's relations with Japan and the United States concerning the adequacy requirement. These case studies, however, reveal more complexity than fits within the de facto unilateral model of EU privacy law diffusion.

B. Different National Approaches

This Section examines the paths taken to reach adequacy in Japan and the United States. The situation in each country was different, and the EU

Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay). The United States is also listed; however, its adequacy finding is "limited to the Privacy Shield framework." *Id.*; *see infra* Section II.B.2.

100 *See Difference Between a Regulation, Directive and Decision*, U.S. MISSION TO EUROPEAN UNION (Dec. 21, 2016), https://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision (noting that a regulation has "binding legal force throughout every Member State and enter[s] into force on a set date in all the Member States" while a directive "lay[s] down certain results that must be achieved but each Member State is free to decide how to transpose directives into national laws").

101 GDPR, *supra* note 29, art. 45(2)(a).

102 For a description of the procedures under the Directive, see CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 175 (2d ed. 2007) [hereinafter KUNER, EUROPEAN DATA PROTECTION LAW]. For the procedures under the GDPR, see GDPR, *supra* note 29, art. 45.

103 *See* European Commission Press Release IP/18/5433, International Data Flows: Commission Launches the Adoption of Its Adequacy Decision on Japan (Sep. 5, 2018).

demonstrated considerable flexibility in response to these varying political and economic landscapes.

1. Japan: Adequate National Law

On January 23, 2019, the EU and Japan reached a mutual adequacy arrangement, which permits personal data to flow freely between the two economies.[104] The highest governance levels of both partners to the agreement had viewed it as a policy priority and as resting on a convergence of the two legal orders. At a G7 summit, the Prime Minister of Japan, Shinzo Abe, and the President of the Commission, Jean-Claude Juncker, pointed to the EU and Japan's shared approach, one based "on an overarching privacy law, a core set of individual rights and enforcement by independent supervisory authorities."[105]

The extensive negotiations and adoption procedures took place over the course of two years. Negotiations began in January, 2017;[106] an agreement in principle was reached in July, 2018;[107] the Commission published a draft adequacy decision in September, 2018;[108] and the European Data Protection Board published its opinion of approval in December, 2018.[109]

The Japan-EU agreement represents a textbook negotiation of an adequacy finding. The GDPR's Article 45(2) provided the basic blueprint for the discussions between the two entities and for the EU's ensuing evaluation of Japanese law.[110] Japan has now entered the EU's coveted

---

104 European Commission Press Release IP/19/421, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019).

105 European Commission Statement 17/1917, Joint Declaration by Mr. Shinzo Abe, Prime Minister of Japan, and Mr. Jean-Claude Juncker, President of the European Commission (July 6, 2017).

106 *See* European Commission Press Release IP/17/16, Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions (Jan. 10, 2017).

107 European Commission Press Release IP/19/421, *supra* note 104; *see* European Commission Statement 18/4548, Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission (July 17, 2018).

108 Graham Greenleaf, *Japan: EU Adequacy Discounted*, PRIVACY LAWS & BUS. INT'L REP., Oct. 2018, at 8, 8.

109 *See Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan*, EUR. DATA PROTECTION BOARD (Dec. 5, 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf.

110 GDPR, *supra* note 29, art. 45(2) (guiding the Commission to take into account multiple factors such as the rule of law and respect for human rights, the existence of one or more independent supervisory authorities in the third country, and the international commitments the third party has entered into).

whitelist of adequate nations.[111] This development is a surprising one. In his 2014 overview of Asian privacy law, Greenleaf titled his chapter on Japan, "The Illusion of Protection."[112] He criticized the Japanese data privacy statute for its limited scope over the private sector, its "easily manipulated exceptions" to its rules concerning the use and disclosure of personal data, its absence of provisions for sensitive information, and its "lack of restriction on data exports."[113] Greenleaf also noted an absence of evidence showing that Japan enforced its data protection law.[114] Rather than an enforceable system for privacy protection, Greenleaf characterized Japanese law as a set of "ritual observances, with little evidence of tangible results."[115]

How did the Japanese go from having an illusory system of data privacy in 2014 to a place on the Commission's list of adequate nations just four years later? The key changes began in 2015 with extensive amendments to Japan's Act on the Protection of Personal Information (APPI).[116] The APPI's amendments altered Japanese law in a fashion that moved it significantly closer to the EU system. These include an expanded definition of sensitive data, greater individual rights, stronger limits on the use of personal data provided to third parties, and enhanced enforcement powers for the Japanese data protection authority, the Personal Information Protection Commission (PPC).[117]

As another novel dimension, the amended APPI contains protection for international transfers of personal data from Japan.[118] In taking this step, Japan adopted a prominent idea of EU data protection law.[119] The amended APPI holds that personal data may not be transferred to a foreign country unless (1) the data subject has given specific advance consent to the

111 Kensaku Takase, *GDPR Matchup: Japan's Act on the Protection of Personal Information*, IAPP (Aug. 29, 2017), https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information.

112 GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES 227 (2014).

113 *Id*. at 263.

114 *Id*.

115 *Id*. at 562.

116 Kojin Jōhō No Hogo Ni Kansuru Hōritsu [Act on the Protection of Personal Information], Law No. 57 of 2003 (Japan), *translated in Amended Act on the Protection of Personal Information (Tentative Translation)*, PERS. INFO. PROTECTION COMMISSION (Dec. 2016), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf [hereinafter APPI].

117 MICHIHIRO NISHI, SKADDEN, ARPS, SLATE, MEAGHER & FLOM, LLP, DATA PROTECTION IN JAPAN TO ALIGN WITH GDPR 2 (2018), https://www.skadden.com/-/media/files/publications/2018/09/quarterly-insights/data_protection_in_japan_to_align_with_gdpr.pdf.

118 *See* APPI, *supra* note 116, art. 24.

119 Nishi, *supra* note 117, at 1 (noting that this is the first time "the EU and a third country have agreed on a reciprocal recognition of the adequate level of data protection").

transfer; (2) the country in which the recipient is located has a legal system deemed equivalent in its privacy protections to the Japanese system; or (3) the recipient undertakes adequate precautionary measures for the protection of personal data specified by the Japanese data protection authority.[120]

The 2015 amendments to the APPI were further bolstered by additional changes that the EU negotiated. The Commission Implementing Decision gives a sense of the deep EU-Japan engagement in reaching the adequacy determination.[121] The ensuing changes to the APPI begin with a set of so-called "Supplementary Rules" issued by the PPC, which have the full effect of legislatively-enacted law.[122] Some of the ensuing protections are limited only to EU-originated personal data.[123] For example, a supplementary protection extends the APPI's list of sensitive data to "personal data received from the EU" concerning an individual's "sex life or sexual orientation or trade-union membership."[124] This change to Japanese data protection extends the protections for "special care-required personal information" in the APPI to the categories recognized as "special categories of personal data" in the GDPR.[125] This coverage is only for personal data from the EU, however, and not for Japanese personal data processed in Japan.[126] The Japanese data protection law has special protection for certain sensitive information to be sure, but this category is

120 APPI, *supra* note 116, art. 24.

121 *See, e.g.*, Commission Implementing Decision (EU) 2019/419, of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information, Annex II, 2019 O.J. (L 76) 1, 44 [hereinafter Commission Implementing Decision on Japan Adequacy] (letter from Yoko Kamikawa, Japan's Minister of Justice, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission).

122 *Id.* Annex I, at 38; Nishi, *supra* note 117, at 1.

123 *See* Commission Implementing Decision on Japan Adequacy, *supra* note 121, ¶ 31. For an overview of the five major substantive changes that will apply only to personal data transferred from the EU under the Supplementary Rules, see Nishi, *supra* note 117, at 2, which summarizes in a chart the heightened protections for EU data: (1) "[s]cope of 'personal information requiring careful consideration,'" (2) "[a]ccess right," (3) "[s]uccession of purpose of use," (4) "[r]e-transfer of EU data subjects' personal data from Japan to foreign countries," and (5) "[a]nonymously processed information."

124 Commission Implementing Decision on Japan Adequacy, *supra* note 121, Annex I, at 39.

125 *Id.*; *see* GDPR, *supra* note 29, art. 9(1); APPI, *supra* note 116, art. 2(3).

126 Commission Implementing Decision on Japan Adequacy, *supra* note 121, Annex I, at 39. Another supplementary protection afforded only to personal data from the EU is that of irreversible anonymization. The APPI defines "anonymously processed personal information" in a way that includes data where re-identification of the individual is still possible. Commission Implementing Decision on Japan Adequacy, *supra* note 121, ¶ 30; *see* APPI, *supra* note 116, arts. 2(9), 36(2). The Supplementary Rules, however, establish that personal data transferred from the EU may only be considered to be anonymously processed "if the personal information handling business operator takes measures that make de-identification of the individual irreversible for anyone, including by deleting processing method etc. related information." Commission Implementing Decision on Japan Adequacy, *supra* note 121, ¶ 31, Annex I, at 43.

defined differently and more narrowly than the GDPR's approach. Hence, Japan agreed essentially to add additional protection for sensitive data received from the EU; this additional protection occurs by expanding the category of covered data for such EU data.

In addition to the Supplementary Rules, the EU-Japan discussions led to a further series of commitments by the Japanese government. These are collected in an Annex to the Commission Implementing Decision which documents the pledge of Japanese authorities to permit the use of personal data for criminal law and national security "only to the extent necessary to the performance of specific duties of the competent public authority as well as on the basis of specific threats."[127] The Annex also details how oversight of data protection is to be carried out in Japan's public sector.[128]

Another aspect of the Implementing Decision is its requirement for periodic reviews of its adequacy finding. The Commission commits to a first review within two years of the agreement's entry into force, followed by subsequent reviews every four years.[129] It requires scrutiny of "all aspects of the functioning of th[e] Decision" with particular attention paid to the application of the Supplementary Rules and to how Japan protects its onward transfers to non-EU countries.[130]

Finally, in an innovative step, the EU-Japan adequacy finding runs in two directions. The two parties established "a reciprocal finding of an adequate level of data protection."[131] Until this moment, the EU's findings of adequacy for foreign data protection regimes concerned only the status of the non-EU country.[132] The EU's findings of adequacy for Argentina, Canada, Israel, New Zealand, or any other so-called "third country" covered only the flow of personal data from the EU to that non-EU entity.[133] In contrast, the EU and Japan have crafted an adequacy decision that recognizes each other's data protection systems.[134] This finding of mutual reciprocity represents a new high point for the diffusion of the EU data protection model. In following the EU approach, Japan will not permit transmission of data from its borders to countries without sufficient data protection.[135] To further this goal, Japan has created a data embargo power

127 Commission Implementing Decision on Japan Adequacy, *supra* note 121, Annex II, at 56.

128 *See id.*

129 *Id.* ¶ 181.

130 *Id.*

131 *EU and Japan Agree on Reciprocal Adequacy*, HUNTON ANDREWS KURTH: PRIVACY & INFO. SECURITY L. BLOG (July 17, 2018), https://www.huntonprivacyblog.com/2018/07/17/eu-japan-agree-reciprocal-adequacy.

132 *Id.*

133 *See id.*

134 European Commission Press Release IP/19/421, *supra* note 104.

135 *See, e.g.*, APPI, *supra* note 116, art. 24 (requiring personal information handling business operators to obtain consent from the data subject for transfers to third parties outside of Japan,

for its national privacy authority.[136]

Mutual reciprocity demonstrates the diffusion of EU ideas. It also illustrates the linkage between economic considerations and data protection. This Article has spoken of GDPR Day, May 25, 2018, as an historic occasion.[137] But an earlier milestone was reached on July 17, 2017. On that day in Tokyo, the EU and Japan announced their joint adequacy decision and their equally ambitious Economic Partnership Agreement.[138] The EU-Japan Economic Partnership Agreement removes a wide range of trade barriers between the two jurisdictions.[139] It is the largest trade deal "negotiated by the EU and will create an open trade zone covering over 600 million people."[140] In a press release issued from Tokyo, the Commission trumpeted the economic aspect of its agreement with Japan and pointed to the creation of "the world's largest area of safe transfers of data based on a high level of protection for personal data."[141] Emphasizing the economic benefits of this arrangement, Věra Jourová, EU Commissioner for Justice, Consumers and Gender Equality, said, "Data is the fuel of [the] global economy and this agreement will allow for data to travel safely between us to the benefit of both our citizens and our economies."[142] The change in Japan from weak to EU-strength data protection is a strategic move that has complemented Japan's growing economic partnership with the EU.

Japan's negotiations with the EU also demonstrate a new model for reconciling international trade law and data protection law. There are important benefits for both parties in making this linkage. Understanding the path-breaking nature of this new approach and why it helps both Japan and the EU requires some historical background.

As Joel Reidenberg pointed out in the 1990s, traditional multilateral trade negotiations, to the extent that they even mentioned privacy, "tilt the balance toward free flows of information."[143] Indeed, there is considerable

unless the third party is in a country with an equivalent standard of data protection).

136 *See id.* art. 42.

137 *See supra* text accompanying notes 21–27.

138 *See EU and Japan Sign Economic Partnership Agreement*, EUR. COMMISSION: DIRECTORATE-GEN. FOR TRADE (July 17, 2018), http://trade.ec.europa.eu/doclib/press/index.cfm?id=1891.

139 *See Fact Sheet: Key Elements of the EU-Japan Economic Partnership Agreement*, EUR. COMMISSION 2–3 (July 6, 2017), http://trade.ec.europa.eu/doclib/docs/2017/july/tradoc_155700.pdf (noting the elimination of more than ninety percent of tariffs on EU exports to Japan and the mitigation of non-tariff barriers, such as Japan's technical and certification procedures, on imported European goods).

140 *EU and Japan Sign Economic Partnership Agreement, supra* note 138.

141 European Commission Press Release IP/18/4501, The European Union and Japan Agreed to Create the World's Largest Area of Safe Data Flows (July 17, 2018).

142 *Id.*

143 Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 295 (1993).

tension between the typical commitment to unhindered data exchanges in trade agreements, including the General Agreement on Trade in Services (GATS)[144] and the regulatory approach of EU data protection to international data transfers.[145] Svetlana Yakovleva and Kristina Irion, two trade scholars, have analyzed whether this disjunction might one day cause arbitrators at the World Trade Organization to reject EU restrictions on data flows through its adequacy approach as being inconsistent with GATS.[146]

In general, the disjunction between trade law and data privacy law rests on a lack of coordination between institutions that negotiate trade and those that negotiate data privacy. On the EU-side, for example, institutions in charge of data protection have not been synced-up, policy-wise, with those negotiating trade agreements.[147] In a normative response to this lack of policy alignment, Yakovleva has called for harmony between future international trade agreements and the EU's protection of privacy while avoiding the subordination of data protection to trade liberalization.[148]

Japan and the EU have now realized such a strategy by simultaneously reaching an ambitious trade agreement and a mutual adequacy finding. On the trade side, the EU-Japan Economic Partnership Agreement has set "the standards for 21st century trade agreements."[149] It goes "beyond trade and tariffs," and "contains clauses pertaining to labor rights, environmental protection and climate change, state-owned enterprises, [and] public procurement."[150] As for data privacy, the separate adequacy finding and related negotiations of changes in Japanese data protection have created a Japan-EU area of free data flows. Data-driven economic sectors in both Japan and the EU can now benefit from the lowering of tariffs through the trade agreement. With personal data a key element of the 21st century economy, Japan and the EU have aligned their normative approaches to

144 General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183.

145 *See* Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUR. DATA PROTECTION L. REV. 191, 192 (2016) ("[P]ersonal data is an essential ingredient of electronic trade in services, to which extensive EU data protection law can be readily perceived as a barrier to free trade.").

146 *See id.* at 208 (concluding that the EU's creation of particular rules for third countries through its adequacy assessments might increase the risk of violating the GATS's national treatment and most favored nation categories).

147 For documentation of this disjunction, see Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows* 6 (OECD Trade Policy Papers, Paper No. 220, 2019).

148 Svetlana Yakovleva, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?*, 17 WORLD TRADE REV. 477, 508 (2018).

149 Andrei Lungu, *Japan and Europe's Triple Partnership*, DIPLOMAT (Feb. 14, 2019), https://thediplomat.com/2019/02/japan-and-europes-triple-partnership.

150 *Id.*; *see also* European Commission Press Release IP/18/6749, EU-Japan Trade Agreement on Track to Enter into Force in February 2019 (Dec. 12, 2018) (highlighting the agreement's focus on standards for labor, environmental protection, and sustainable development).

both trade and data protection. The point could not be clearer: Data protection is an essential element of international business.

2. The United States and the Privacy Shield: Private Sector Opt-in

The United States has never formally sought an adequacy determination from the Commission. According to Christopher Wolf, the American reluctance to request an adequacy determination follows from the "well-understood outcome [of such a request]: request denied."[151] Instead, the United States and the EU have settled on a strategy around à la carte findings of adequacy. Before the Safe Harbor[152] and independent of its negotiations with the United States, the EU had already developed two such paths: standard contractual clauses[153] and binding corporate rules (BCRs).[154]

The standard contractual clauses establish approved rules for transmitted data.[155] If used, these clauses must be signed for each transfer by the sending entities in the EU and the receiving entities in the United States.[156] In contrast, "[BCRs] are internal rules for data transfers within multinational organizations."[157] The EU describes them as being "like a code of conduct" to cover a company's data practices worldwide.[158] As Christopher Kuner explains, BCRs permit organizations to benefit from "a more integrated, holistic approach" rather than one that must be determined for each transfer of information.[159] BCRs make the entire organization a kind of "safe haven" in which personal data can be transferred internally without concerns for national borders.[160]

---

151 Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227, 229 (2013).

152 *See infra* Section II.B.2.a.

153 Commission Decision 2010/87, of 5 Feb 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5 [hereinafter Standard Contractual Clauses].

154 GDPR, *supra* note 29, art. 47 (incorporating binding corporate rules (BCRs) into the GDPR); *see also Binding Corporate Rules (BCR)*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en (last visited Apr. 8, 2019) (describing the purpose of BCRs and the process of approval for companies).

155 *See* Standard Contractual Clauses, *supra* note 153, art. 1 ("The standard contractual clauses . . . are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.").

156 *See id.*, Appendix 1, at 16–17 (requiring completion by and signature of both the data exporter and data importer).

157 *Binding Corporate Rules (BCR)*, *supra* note 154.

158 *Id.*

159 KUNER, EUROPEAN DATA PROTECTION LAW, *supra* note 102, at 219.

160 *Id.*

Standard contractual clauses and BCRs are open to any entity in a country not on the whitelist of adequate nations.[161] As these two options illustrate, the EU has long made clear that adequacy is to be judged by the actual practices of data processing entities. Regardless of the domestic, non-EU law that formally regulates a foreign entity, an organization outside the EU can achieve adequacy if it provides sufficient data protection for transmitted data. These two paths to adequacy, the contractual clauses and BCRs, are open to U.S. companies, but they are generally viewed as being relatively costly and inflexible measures. The standard contractual clauses do not fit each type of data transfer, must be used without change, and are considered as imposing terms that "are relatively onerous to meet and can lead to high administrative costs."[162] As for BCRs, such an internal program requires international coordination within a corporation throughout its global operations and then formal approval by an EU data protection authority.[163] In Kuner's cautionary assessment, "BCRs raise significant challenges . . . since the approval process can be lengthy, and implementation can be expensive and difficult for all but large multinationals."[164]

The Directive and the GDPR also foresee other approaches and therefore permit limited adequacy findings. In the GDPR, for example, there is an allowance for a finding of adequacy not only for a "third country," but also for "a territory or one or more specified sectors within that third country."[165] In one such limited adequacy finding for a single sector, the EU negotiated an agreement with the U.S. government over airline transfers of Passenger Name Records from the EU to the United States.[166]

More broadly than these measures, the EU and United States have developed two programs of voluntary private sector compliance. These are, first, the Safe Harbor[167] (2000 to 2015), and later, the Privacy Shield[168]

---

161 GDPR, *supra* note 29, art. 46(1)–(2) (including BCRs and standard contractual clauses in the list of appropriate safeguards available to entities in third countries or international organizations that lack an adequacy determination).

162 Casalini & López González, *supra* note 147, at 20.

163 *See Binding Corporate Rules (BCR)*, *supra* note 154 (describing the process of approval, including the drafting of the BCRs, which must comply with the Article 29 Working Party's requirements, and the approval of all data protection authorities). For the most recent guidance on BCRs from the Article 29 Working Party, see *Working Document of Article 29 Working Party on Setting Up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules* (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49725.

164 KUNER, EUROPEAN DATA PROTECTION LAW, *supra* note 102, at 220.

165 GDPR, *supra* note 29, art. 45(1).

166 Agreement on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, EU-U.S., Dec. 14, 2011, T.I.A.S. No. 12-701.

167 Commission Decision 2000/520/EC, of 26 July 2000 Pursuant to Directive 95/46/EC of

(2016 to present). In these two bilateral agreements, the EU and United States did not proceed through formal treaty-making, draw on existing international trade agreements, or create any kind of legal instrument to immediately bind private companies. Rather, these two arrangements agreed on a streamlined list of substantive EU principles for American companies to follow voluntarily.[169] This Section first focuses on the Safe Harbor and the Privacy Shield. It then considers the key role played by the Court of Justice of the European Union through its decision in *Schrems v. Data Protection Commissioner*.[170]

a. The Safe Harbor

Faced with the EU's view that the United States was failing to provide adequate data protection,[171] the United States engaged the EU in discussions regarding a possible solution to allow international data flows to continue from the EU to the United States. In 2000, following multi-year bilateral negotiations, the Commission and the U.S. Department of Commerce agreed on the Safe Harbor Principles.[172] In the resulting document, there was something for both sides.

As a starting point, Congress and the U.S. government did not wish to enact an omnibus, EU-style privacy law.[173] Indeed, leading U.S. tech

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 U.S. Department of Commerce, Annex I, 2000 O.J. (L 215) 7 [hereinafter Safe Harbor Decision]; *see* Issuance of Safe Harbor Principles and Transmission to European Commission; Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 (Sept. 19, 2000); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).

168 *See* U.S. DEP'T OF COMMERCE, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES (July 12, 2016), https://www.privacyshield.gov/privacy-shield-principles-full-text [hereinafter EU-U.S. PRIVACY SHIELD FRAMEWORK].

169 *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 5, 9 (2016) (describing how negotiations surrounding both agreements ultimately resulted in principle-based, opt-in systems to regulate data transfers).

170 *See infra* note 204 and accompanying text.

171 *See Opinion 1/99 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government* (Jan. 26, 1999), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf (stating in reference to U.S. privacy law that "the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection" for data transferred from the EU).

172 *See* Henry Farrell, *Negotiating Privacy Across Arenas: The EU-U.S. "Safe Harbor" Discussions*, *in* COMMON GOODS: REINVENTING EUROPEAN AND INTERNATIONAL GOVERNANCE 105, 105–26 (Adrienne Héritier ed., 2002) [hereinafter Farrell, *Negotiating Privacy Across Arenas*] (examining the negotiations between the United States and the EU over the Safe Harbor Principles).

173 *See id.* at 109 ("The United States administration has concluded that regulation is inappropriate, given how swiftly e-commerce is evolving and has instead sought to encourage

companies of that era were strongly opposed to such a law.[174] The belief was that governmental regulation of privacy would inevitably stifle the development of commerce in cyberspace.[175] As a Vice President of American Express wrote in 1997, "We believe that government regulation of privacy on the Internet and other online areas is very risky given the rapid changes in this new technology."[176] The Clinton administration adopted this perspective and favored industry self-regulation.[177] In 1997, President Clinton announced *A Framework for Global Electronic Commerce*,[178] which stated, "The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes."[179]

In allowing U.S. companies to voluntarily accept the Safe Harbor Principles, the U.S. government found a way both to promote self-regulation and to permit data transfers to continue to the United States. There was also a sense of urgency for U.S. negotiators; in the 1990s, the commercial internet had emerged, and U.S. companies were developing business models that relied on personal data.[180]

---

self-regulation in areas such as privacy, in the belief that self-regulation would be more flexible and responsive.").

174 In reaction to the possibility of regulation through legislation, several major companies in 1998 banded together to form the Online Privacy Alliance, which focused on promoting self-regulation as an alternative to possible legislation. *See id.* at 119. Members of the Online Privacy Alliance included companies such as Apple, AT&T, Dell, eBay, and Microsoft. Letter from Tim Lordan, Online Privacy All., to Jane Coffin, Nat'l Telecomm. and Info. Admin. (July 2, 1998), https://www.ntia.doc.gov/legacy/ntiahome/privacy/mail/disk/PrivAlliance.html.

175 *See* Peggy H. Haney, *Case Study of American Express' Privacy Principles: Why and How They Were Adopted, the Choices Involved and a Cost-Benefit Analysis*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 209, 213 (U.S. Dep't of Commerce ed., 1997) ("Regulation could promote one technology over another and act as a barrier to the full realization of the benefits of commerce in cyberspace.").

176 *Id.*

177 *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 774–75 (1999) (noting the Clinton Administration's continued support for self-regulation of fair information practices and general reluctance to pass legislation); *see also* Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 113–14 (1995) (criticizing the U.S. approach to information privacy as based on "[t]he religion of self-regulation").

178 Message to Internet Users on Electronic Commerce, 2 PUB. PAPERS 901, 901 (July 1, 1997).

179 THE WHITE HOUSE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 18 (1997) [hereinafter THE WHITE HOUSE]. For a discussion of the U.S. privacy landscape at the time, see Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 27–28 (2000).

180 *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 516, 523 (1995) (identifying the burgeoning direct marketing industry and the creation of lucrative marketing profiles as dependent on personal data); Shaffer, *supra* note 179, at 44–46 (describing the pressure surrounding the negotiations from U.S. firms to protect self-regulation and from the EU, which refused to recognize the status quo U.S. approach as adequate).

The Safe Harbor promoted self-regulation by leaving it up to firms to decide whether or not to follow its principles through an opt-in system. In this fashion, as Henry Farrell notes, the U.S. government strategically introduced the hands-off concept of self-regulation, the leading ideology of cyberspace in the 1990s, into international privacy discourse.[181] Beyond its basic opt-in architecture, and as a further example of its promotion of self-regulation, the Safe Harbor permitted organizations to use third-party private organizations as an element of their oversight of compliance.[182]

On the EU side, negotiators recognized that political realities in the United States made the enactment of an omnibus U.S. privacy statute unlikely.[183] Moreover, member states within the EU had not fully harmonized their national laws as required by the Data Protection Directive, the 1995 precursor to the GDPR.[184] Joel Reidenberg concisely summed up the state-of-play in the mid-1990s: "The prospect of change in US law seemed remote and the European Commission would have serious political difficulty insisting on an enforcement action against data processing in the United States prior to the full implementation of the European Directive within the European Union."[185] The Safe Harbor provided a way out of this potential impasse while simultaneously protecting EU citizens' data. It also allowed the EU to safeguard the economies of its member states. As Stephen Weatherill has observed, "Trade is the EU's business."[186] Building on its roots in the European Coal and Steel Community of 1951, the modern EU wishes to serve as a motor for economic prosperity for its member states and the Eurozone.[187] The EU

181 *See* Henry Farrell, *Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement*, 57 INT'L ORG. 277, 290–91 (2003) [hereinafter Farrell, *Constructing the International Foundations of E-Commerce*] (finding that U.S. officials intended to promote self-regulation as the strategy to protect privacy in the international sphere to align with U.S. domestic policy); *see also id.* at 295 (noting the success of the United States in convincing EU representatives to adopt self-regulation measures).

182 For example, U.S. companies were able to use private companies, such as BBBOnline or TRUSTe, to resolve consumer complaints and to deal with other aspects of first-line enforcement measures. *Id.* at 287; *see* KUNER, EUROPEAN DATA PROTECTION LAW, *supra* note 102, at 182–83 (describing the dispute resolution and enforcement mechanisms available to companies).

183 *See* Farrell, *Negotiating Privacy Across Arenas*, *supra* note 172, at 111 (describing how the EU's initial insistence on a comprehensive legislative solution gave way to acceptance of a voluntary solution that granted adequacy determinations to firms on an opt-in basis).

184 Council Directive 95/46/EC, *supra* note 86.

185 Reidenberg Statement, *supra* note 20, at 72.

186 STEPHEN WEATHERILL, LAW AND VALUES IN THE EUROPEAN UNION 407 (2016).

187 *See id.* at 395 ("The original European Communities were heavily focused on achieving economic reform and growth in part because of the vital need to reshape and reenergize shattered Europe . . . ."); *The EU in Brief*, EUR. UNION, https://europa.eu/european-union/about-eu/eu-in-brief_en#from-economic-to-political-union (last updated Mar. 28, 2019) (describing "sustainable development based on . . . a highly competitive market economy" and the enhancement of "economic . . . cohesion and solidarity among EU countries" as goals of the EU).

has therefore sought to promote not only data protection but also the free flow of data. As the Data Protection Directive states, "[C]ross-border flows of personal data are necessary to the expansion of international trade . . . ."[188] Achieving this goal means finding a way to facilitate trade with the United States, the EU's most important external trade partner.[189]

The digital single market strategy[190] of the EU provides insights into the linkage of the free flow of data to trade. This current policy program aims to diminish a variety of barriers "to unlock online opportunities."[191] The purpose of the digital single market is to guarantee free movement of data so that "citizens and businesses can seamlessly and fairly access online goods and services, whatever their nationality, and wherever they live."[192] Specific goals include modernizing copyright, strengthening cybersecurity, abolishing roaming charges for Europeans within the EU, and increasing access to broadband.[193] The EU also seeks to have a high level of privacy for all electronic communications and to promote cross-border flows of personal data.[194] In short, the flow of global data is an important part of the EU's plan to promote a global information economy.[195]

As for the contents of the Safe Harbor, it contained seven key principles of data privacy law. These were (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement.[196] All of these principles can be found, at least to some extent, in different kinds of U.S. information privacy law, but the Safe Harbor put them into a single document and expressed these concepts in a fashion reflective of EU data protection law.[197] By 2015, some 4,500 U.S. companies had publicly affirmed their following of the Safe Harbor and

188 Council Directive 95/46/EC, *supra* note 86, recital 56, at 36.

189 *See* WEISS & ARCHICK, *supra* note 169, at 4 ("The United States and the EU remain each other's largest trade and investment partners. In 2013, total U.S.-EU trade in goods and services amounted to $1 trillion and U.S. FDI in EU totaled $2.4 trillion . . . .").

190 *Digital Single Market*, EUR. COMMISSION, https://ec.europa.eu/commission/priorities/digital-single-market_en (last visited Apr. 7, 2019).

191 *Id.*

192 *Id.*

193 *Id.*

194 *See* European Commission Press Release IP/17/16, Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions (Jan. 10, 2017) (announcing new proposals that increase privacy protections for electronic communications while still facilitating data exchange).

195 *See* Schwartz & Peifer, *supra* note 7, at 130 (describing the EU's goal to promote the free flow of data among member states).

196 *Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks*, FED. TRADE COMMISSION (Dec. 2012), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

197 *See* Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 85, at 1981 (describing the Safe Harbor as "a negotiated mixture of EU-U.S. standards . . . that ends somewhat closer to the EU version rather than the U.S. version of privacy norms").

listed their names on the official site for the agreement, which the U.S. Department of Commerce maintained.[198]

In hindsight, the Safe Harbor negotiators on both sides acted strategically at just the right time. By providing U.S. companies a path around potentially counterproductive EU data embargo orders, the resulting agreement allowed the EU and United States to enjoy the benefits of transatlantic digital products and services. The Safe Harbor also brought EU data protection into the mainstream of a global discussion about privacy regulation as the commercialization of the internet was beginning.[199]

On the EU side, however, controversy accompanied the Commission's judgment that the Safe Harbor met the adequacy standard. In 2000, the European Parliament passed a non-binding resolution rejecting the Safe Harbor.[200] In prescient testimony to the U.S. Congress in 2001, moreover, Reidenberg predicted that the Safe Harbor was vulnerable to collapse.[201] Speaking before the House of Representatives, he characterized the Safe Harbor as offering only "false hopes" and stated that it dramatically weakened European standards, in particular by containing exceptions not present in European law and by watering down requirements for redress of privacy violations.[202]

b. The Demise of the Safe Harbor and Birth of the Privacy Shield

In 2015, the United States and the EU were well underway in negotiations to modify the Safe Harbor.[203] A decision of the European Court of Justice (CJEU) in October 2015 upended any plans, however, for a modestly revised Safe Harbor 2.0. In *Schrems v. Data Protection Commissioner*, the CJEU voided the Safe Harbor Agreement.[204] This result strengthened the hand of the EU in its high-stake negotiations with the

198 WEISS & ARCHICK, *supra* note 169, at 5–6.

199 The EU's regulatory model and the Safe Harbor Agreement already represented a considerable movement away from the U.S. minimalist approach towards information privacy on the internet by the Clinton Administration, circa 1997. *See* John M. Broder, *Ira Magaziner Argues for Minimal Internet Regulation*, N.Y. TIMES (June 30, 1997), https://www.nytimes.com/1997/06/30/business/ira-magaziner-argues-for-minimal-internet-regulation.html. For the Magaziner Report, see THE WHITE HOUSE, *supra* note 179.

200 *Report on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles*, at 10 (June 22, 2000), www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/03_ereport2000pe_285929_/03_epreport2000pe_285929_en.pdf.

201 Reidenberg Statement, *supra* note 20, at 75.

202 *Id.* at 71, 74.

203 WEISS & ARCHICK, *supra* note 169, at 1.

204 Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 ¶¶ 96–98 (Oct. 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

United States.[205]

In *Schrems*, the CJEU found that the Safe Harbor fell short of the requirements of the Data Protection Directive, as read in light of the European Charter.[206] In particular, and in light of leaks from Edward Snowden regarding the surveillance activities of the U.S. National Security Agency, the CJEU found that the Safe Harbor permitted "national security, public interest, or law enforcement requirements" to "have primacy" over the data protection principles of the transnational agreement.[207] Moreover, the CJEU faulted the Safe Harbor for "permitting the public authorities to have access on a generalised basis to the content of electronic communications."[208] Such an approach, it said, "must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter [of Fundamental Rights of the European Union]."[209]

This decision also settled questions regarding the meaning of the adequacy standard established by the Data Protection Directive in 1995. The *Schrems* Court declared that the adequacy standard of European data protection called for an "essentially equivalent" level of protection in a third-party nation.[210] Henceforth, there could be no doubt as to the relationship between the "adequacy" of protection required for transfers of personal data *from* the EU compared to the "equivalency" of protection required *between* EU member states. Moreover, the *Schrems* decision constitutionalized the "adequacy" standard as well as other aspects of EU data protection law by grounding its opinion in cornerstone documents of European integration, most notably the Charter of Fundamental Rights of the European Union, Articles 7 and 8.[211] *Schrems* gives the CJEU the ultimate authority over EU decisions concerning international data transfers.

Finally, in detailed comments in its *Schrems* decision, the CJEU provided a roadmap for EU negotiators by making clear its expectations for any future agreement with the U.S post-*Schrems*. By grounding these requirements in EU constitutional law, this decision offers further proof, in Alec Stone Sweet's words, of how "European policy-making has been

---

205 *See* Schwartz & Peifer, *supra* note 7, at 160 ("In the aftermath of *Schrems*, the ongoing negotiations between the Commission and U.S. Department of Commerce took on new urgency. 'Safe Harbor 2.0' was a brand without a future.").

206 Case C-362/14, *Schrems*, ¶ 107(1).

207 *Id.* ¶¶ 30, 86.

208 *Id.* ¶ 94.

209 *Id.*

210 *Id.* ¶¶ 73–74, 96.

211 *Id.* ¶ 107(1); *see* Charter of Fundamental Rights of the European Union, art. 7–8, 2000 O.J. (C 364) 1 (articulating the principles relied on in the *Schrems* decision).

judicialized."[212] *Schrems* makes clear, for example, that a U.S.-EU agreement could not restrict the power of the national DPAs to initiate investigations of international data transfers.[213] If the Commission took such a step, it would exceed the powers of the Commission under EU law.[214]

Once the CJEU struck down the Safe Harbor, U.S. companies faced more complicated and costly alternatives for international data transfers, such as standard contractual clauses and BCRs.[215] In recognition of the ongoing transatlantic negotiations, however, European data protection authorities temporarily agreed not to prosecute companies who continued to use the Safe Harbor agreement post-*Schrems*.[216] By early 2016, negotiations between the EU and United States for a successor agreement proved successful, and the EU and U.S. Department of Commerce released the details of the Privacy Shield.[217] Following demands from the European Parliament in March 2016, the Department of Commerce strengthened some aspects of the agreement and received final approval from the Parliament in July 2016.[218] The official implementation of the Privacy Shield began on August 1, 2016.[219]

The Privacy Shield does not represent a complete break with the past. For one thing, it largely adopts the same seven principles as found in the Safe Harbor.[220] The considerable overlap between the Privacy Shield and Safe Harbor Principles means a continuity in basic vocabulary and orientation, which offers potentially lower compliance costs for the U.S. companies that agreed to the earlier arrangement. But the Privacy Shield also strengthens the Safe Harbor Principles in notable ways and, thereby, further develops transatlantic data privacy norms.

Alterations to the Safe Harbor Principles vary from minor to major. To concentrate on the latter, the Privacy Shield makes dramatic changes to

---

212 ALEC STONE SWEET, GOVERNING WITH JUDGES: CONSTITUTIONAL POLITICS IN EUROPE 1 (2000) (emphasis in original).

213 Case C-362/14, *Schrems*, ¶¶ 103–04.

214 MARK DAWSON, THE GOVERNANCE OF EU FUNDAMENTAL RIGHTS 70 (2017).

215 *See supra* text accompanying notes 153–160.

216 SHARA MONTELEONE & LAURA PUCCIO, EUROPEAN PARLIAMENTARY RESEARCH SERV., PE 595.892, FROM SAFE HARBOUR TO PRIVACY SHIELD 12 (2017), http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf.

217 *Id.* at 17.

218 *Id.* at 20–21.

219 *Id.* at 21.

220 *See* WEISS & ARCHICK, *supra* note 169, at 9 (describing how the Privacy Shield includes and expands upon the principles of notice, choice, security, data integrity, access, and enforcement); *see also supra* note 196 and accompanying text (describing the same principles as the foundation of the Safe Harbor).

the Safe Harbor's principle of "Enforcement."[221] It reconfigures this concept as "Recourse, Enforcement and Liability."[222] While repeating much of the Safe Harbor's language, it places important additional obligations on organizations to "respond expeditiously to complaints regarding compliance with the [Privacy Shield] Principles referred by EU Member State authorities through the Department" as well as in other aspects of the enforcement process.[223] These include placing liability on a Privacy Shield organization for damages that follow from onward transfers to a third party, who then processes "such personal information in a manner inconsistent with the Principles."[224] Moreover, it increases the individual's ability to access her personal data while also limiting the availability of consent as a basis for data processing, thereby creating a safeguard against individuals being pressured to make choices to their detriment.[225]

Beyond these changes to the Safe Harbor Principles, new institutional commitments by the United States accompanied the Privacy Shield. These included an official statement by the Office of the Director of the National Intelligence that the U.S. intelligence apparatus would not engage in mass surveillance of data transferred under the Privacy Shield.[226] These assurances are important in light of the CJEU's concerns in *Schrems* about the United States engaging in supposedly indiscriminate mass surveillance of EU data.[227] Moreover, the Commission's implementing decision of July 12, 2016 emphasized the requirement of periodic reviews of its adequacy finding.[228] Looking to the future, the function of many elements of the current framework will depend on future decisions as the EU deploys the mechanisms built into the Privacy Shield for transatlantic consultations.

III
THE INFLUENCE OF EU DATA PROTECTION

This Part argues that the case studies cast doubt on the ideas that the

221 Safe Harbor Decision, *supra* note 167, Annex I, at 12.

222 EU-U.S. PRIVACY SHIELD FRAMEWORK, *supra* note 168, Section II.7.

223 *See id.* Section II.7(b)–(d) (describing a variety of enforcement procedures intended to ensure compliance with the Privacy Shield).

224 *Id.* Section II.7(d).

225 *See id.* Sections II.6, III.8 (explaining the access principle).

226 Letter from Robert S. Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, to Justin S. Antonipillai, Counselor, U.S. Dep't of Commerce, and Ted Dean, Deputy Assistant Sec'y, Int'l Trade Admin. 18 (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F.

227 *See* Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 ¶¶ 22, 25 (Oct. 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

228 Commission Implementing Decision (EU) 2016/1250, of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, ¶ 145, 2016 O.J. (L 207) 1 [hereinafter Commission Implementing Decision on Privacy Shield Adequacy].

EU exercises unilateral power and reaches only de facto results. Instead, they demonstrate that the EU employs a broad set of strategies that have encouraged the spread of its data protection law. Beyond these strategies, the EU has benefited both from developing concepts that have proved successful in a global marketplace of ideas and from elaborating a highly transplantable legal model.[229]

A. Lessons from the Case Studies

In Japan, the process of reaching an adequacy agreement proved to be neither unilateral nor de facto. Instead of a unilateral imposition, Japan chose to engage in bilateral negotiations with the EU and create a reciprocal agreement that resulted in the world's largest zone for free data exchanges.[230] Furthermore, the result is de jure, not de facto law. The commitments were carefully documented in the APPI and the Annexes to the Commission Implementing Decision.[231] Moreover, this result does not seem to have followed Bradford's timeline, which predicts that widespread adoption by export-oriented domestic companies occurs first and is then followed by their lobbying of the national government.[232] Rather, Japan's choice has been a qualitative one. It affirmatively chose a system similar to and compatible with EU data protection law. It did so based, in part, on a judgment regarding the merits of competing data privacy regulatory systems.

Behind this decision is not only Japan's assessment of its economic interests. Just as Japan adopted Germany's civil code in 1896 after considering other international approaches, it chose to follow the path of EU law in this century based on a value assessment and modified Japanese law accordingly.[233] The Japan-E.U. agreement further represents a coordination of broader trade negotiations with data protection agreements. This linkage demonstrates the benefits to both parties through the creation of a zone for data trade.

Regarding the United States, the EU proved open to bilateral deal making in its negotiations around the Safe Harbor and the Privacy Shield. The Safe Harbor and the Privacy Shield modified classic EU principles just

229 *See infra* Section III.B.

230 European Commission Press Release IP/18/6749, *supra* note 150.

231 *See* Commission Implementing Decision on Japan Adequacy, *supra* note 121, ¶ 4 ("These conditions are laid down in the Supplementary Rules (Annex I) adopted by the Personal Information Protection Commission . . . and the official representations, assurances and commitments by the Japanese government to the European Commission (Annex II).").

232 Bradford, *supra* note 47, at 6.

233 Zentaro Kitagawa, *Development of Comparative Law in East Asia*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 236, 239–42 (Mathias Reimann & Reinhard Zimmermann eds., 2006); *see* European Commission Press Release IP/18/6749, *supra* note 150.

enough to make the results tolerable on the American side of the Atlantic, while remaining defensible in Brussels and within member states.[234] Rather than a unilateral exertion of power, these negotiations show striking flexibility and cooperation on the EU's part. This flexibility reflects a realization that the United States is the largest trading partner of the EU.[235] In light of the EU's goal of promoting successful external trade for its single market bloc of member states, the United States represents its most valuable economic relationship.

Moreover, while the voluntary participation of U.S. companies in the resulting agreements can be seen as a kind of de facto result, the U.S. government has made a series of formal commitments in the Privacy Shield, which represent de jure law.[236] Here, too, the rise of de jure law has not followed Bradford's predicted sequence. Rather, the original Safe Harbor Agreement was developed *before* U.S. companies had widely adopted EU-style data protection, or even had great exposure to it.[237] U.S. companies had not lobbied for it, and the idea itself came from Ambassador David Aaron, the key U.S. negotiator of this agreement, who once explained that it "just popped into [his] head" as he sat in the office of his EU counterpart, John Mogg, one day in early 1998.[238]

This approach has also been a great success with the U.S. private sector. As U.S. Commerce Secretary Ross noted in October 2018, "[I]t has taken only 24 months for the Privacy Shield to enroll the same number of participants as it took the Safe Harbor 13 years to achieve."[239] Part of this rapidity in adoption can be attributed to the existing familiarity of U.S. companies with the underlying internal steps and external processes involved in this kind of self-certification program. The many years of experience of American privacy professionals with the Safe Harbor provided this experience. More broadly, the impressive rate of adoption represents proof of the value of such a mechanism for U.S. companies.

---

234 *See* Farrell, *Constructing the International Foundations of E-Commerce*, *supra* note 181, at 296–97 (describing how the Safe Harbor "does not directly require the United States to change how it regulates e-commerce and privacy"); Schwartz & Peifer, *supra* note 7, at 164–65 (explaining that while the Privacy Shield moved the needle closer to EU data privacy principles, "the bottom line for the free flow of data was acceptable" to the United States).

235 *See supra* note 189 and accompanying text.

236 *See* WEISS & ARCHICK, *supra* note 169, at 9–10 (detailing the U.S. Department of Commerce's commitment to enforcing the Privacy Shield principles and the commitment by U.S. officials to limit use of EU citizens' personal data).

237 *See* Farrell, *Constructing the International Foundations of E-Commerce*, *supra* note 181, at 285.

238 *Id.* at 292.

239 Wilbur L. Ross, U.S. Sec'y of Commerce, Remarks at the Second Annual Review of the EU-U.S. Privacy Shield in Brussels, Belgium (Oct. 18, 2018), https://www.commerce.gov/news/speeches/2018/10/remarks-commerce-secretary-wilbur-l-ross-second-annual-review-eu-us.

Although the EU's design here is one that permits structured self-regulation and not direct regulation of U.S. companies, it has effectively changed the data privacy practices of many organizations in the United States for processing EU data and even non-EU data. The EU has worked with regulators, and also reached around regulators in the United States by making its principles available for voluntary adoption. Thus, the two case studies suggest different lessons about how Brussels regulates data privacy. These case studies also build on each other to suggest lessons about the power of the adequacy requirement and the EU's regulatory capacity. This Section now turns to these themes.

1. Negotiating and the Adequacy Requirement

While all roads may lead to Brussels, there are many paths to achieving adequacy, and the EU has demonstrated a wide range of flexible approaches with regard to this standard. For some critics, it may even be too accommodating. That was the CJEU's view in *Schrems* regarding the EU-U.S. Safe Harbor.[240] Concerning Japan, Greenleaf has expressed his doubts about the EU-Japan adequacy agreement in light of Japan's weak track record for enforcement. In particular, he asks, "Should an adequacy assessment take on trust that there will be future stronger enforcement?"[241] From another perspective, however, the EU is not relying on trust, but on its ability to obtain future improvements in Japan's enforcement, if needed, through the bilateral review process that is built into the EU-Japan adequacy agreement.[242]

The case study of Japan also demonstrates that, over time, the EU has been able to learn from past negotiations and, in general, to raise the bar for its adequacy test. In 2003, the Commission found Argentina to have adequate data protection in a brief four-page decision.[243] To some observers, this action was proof of the arbitrary nature of the EU's whitelist for data transfers.[244] Others consider the adequacy finding for Argentina as that country's reward for adopting an EU-style data protection law at a time when such legislation had not yet spread throughout Latin America, let

---

240 Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 ¶¶ 96–98 (Oct. 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

241 Graham Greenleaf, *Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles* 10 (Univ. of N.S.W. Law, Research Paper No. 18–53, 2018), https://ssrn.com/abstract=3219728.

242 *See supra* text accompanying notes 129–130.

243 Commission Decision 2003/490/EC, of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina, art. 1, 2003 O.J. (L 168) 19.

244 *See, e.g.*, Wolf, *supra* note 151, at 240–41 (comparing the Argentina adequacy opinion with the European Commission's refusal to issue an adequacy decision for Burkina Faso despite some similarities between the two).

alone the world.[245] In 2017, the Commission acknowledged its attention to the possible influence on other lands of the adoption by a non-EU member state of data protection.[246] In starting "a dialogue on adequacy," the Commission noted it would take into account "the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region."[247]

Japan certainly has the potential to serve as such a model for other Asian countries deciding on a privacy regime. Nevertheless, Japan faces a more complicated and, in general, more onerous path to adequacy than Argentina did over a decade earlier. The latest development in this saga is that both the Parliament and European Data Protection Board have issued opinions asking for "further clarifications," that is, changes to the agreement between the EU and Japan.[248] These views are likely to lead to modifications of the draft adequacy agreement between the Commission and Japan. At the same time, however, other countries in the Asian Pacific region still view an adequacy determination from the EU as the gold standard for ensuring data flows.[249] Korea is now in the process of negotiations to join the EU's whitelist as well.[250]

In sum, the adequacy requirement has given the EU an important point of leverage in negotiations, but its negotiators have not exercised unilateral power. Rather, they have flexibly assessed the adequacy of different legal systems as it suits the EU's goals at the time. Future negotiations are also built into recent agreements and will take place, for example, through bilateral reviews set at intervals with Japan and the United States respectively.[251]

---

245 *See* CHRISTOPHER KUNER, TRANSBORDER DATA FLOW REGULATION AND DATA PRIVACY LAW 66 (2013) (stating, diplomatically, that "members of the Article 29 Working Party have told the author that politics entered into that group's decision to approve Argentina as providing an adequate level of protection"); *Adequacy Decisions*, *supra* note 99.

246 European Commission Memo/17/15, Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers (Jan. 10, 2017).

247 *Id.*

248 Gabor Gerencser, *Japan's Long Road for Adequacy Under the GDPR*, IAPP (Dec. 18, 2018), https://iapp.org/news/a/japans-long-road-for-adequacy-under-the-gdpr.

249 *See* Greenleaf, *supra* note 112, at 32 ("[T]he EU Directive to Asian countries . . . embodies the 'European standards' for data privacy which have been and continue to be very influential in the development of national data privacy laws in Asia and elsewhere outside Europe, because of the aspiration of countries to adopt what is perceived as international 'best practice' . . . .").

250 Daniel R. Stoller, *South Korea Privacy Law Changes May Help EU Data Transfer Talks*, BLOOMBERG L. (Feb. 22, 2019, 11:39 AM), https://news.bloomberglaw.com/privacy-and-data-security/south-korea-privacy-law-changes-may-help-eu-data-transfer-talks.

251 *See supra* text accompanying notes 129–132.

2. Regulatory Capacity and Institutional Interplay

One of the most striking themes of this Article's case studies concerns the EU's regulatory capacity. Bradford is correct to emphasize this factor as a major element of her Brussels Effect.[252] The EU's regulatory capacity must be understood, however, as resting on a complex interplay among its institutions beyond the Commission, the executive body of the EU. In his examination of the protection of data protection interests in the EU, Mark Dawson argues that there is a "significant dispersion of power within the EU legislative process – a dispersal that allows [fundamental rights] considerations ignored by some institutions to be brought to light by others."[253]

To illustrate this dispersal of power, we can consider the data protection authorities (DPAs) in the member states, the European Data Protection Supervisor (EDPS), and the European Data Protection Board (EDPB). The DPAs have an essential role under the GDPR.[254] For example, these officials must approve companies' use of BCRs to ensure that all data transfers within a corporate group meet EU standards.[255]

The GDPR also grants important roles to the EDPS and the EDPB. The EDPS Supervisor acts as the EU's data protection officer with authority over data processing by the EU's own institutions.[256] In addition, this official advises the EU on policy matters and works with the national DPAs to improve the consistency of data protection throughout EU member states.[257] As for the EDPB, it is an important body whose extensive tasks are set out in Articles 68–76 of the GDPR. A member from each national DPA sits on the EDPB with the chief task of "ensur[ing] the consistent application" of the GDPR.[258] To further this goal, it issues guidelines and recommendations, and provides the Commission with its opinion regarding the adequacy of the level of protection in third countries.[259] The Board also plays a key role as part of the GDPR's "consistency mechanism,"[260] which allows it, in some cases, to issue binding decisions regarding certain actions by national DPAs.[261]

As part of this institutional interplay, the EU has been open to ideas

252 *See* Bradford, *supra* note 47, at 5.
253 Dawson, *supra* note 214, at 141.
254 *See supra* text accompanying notes 67–74.
255 GDPR, *supra* note 29, art. 47.
256 GDPR, *supra* note 29, art. 51(1). For more on the EDPS, see its website at https://edps.europa.eu.
257 *Id.* arts. 57(1)(c), (g), 61.
258 *Id.* art. 70(1).
259 *Id.* art. 70 (1)(d), (f)–(m), (s).
260 *Id.* art. 63.
261 *Id.* art. 65(1). For more information on the EDPB, see its website at https://edpb.europa.eu/edpb_en.

from outside jurisdictions as well. For example, the GDPR contains privacy innovations from other countries. These include a requirement of data breach notification, an idea first embodied in a California statute from 2002 and now found in all fifty American states.[262] From the Children's Online Privacy Protection Act of 1998, the GDPR took the requirement of special protection for the personal data of children, including a requirement of parental consent.[263] From Canada, and, in particular, from the province of Ontario and the tireless policy entrepreneurship of data protection commissioner Ann Cavoukian, the GDPR adopted the principle of privacy by design.[264] The idea of privacy by design is to integrate privacy and security from the earliest stages of the planning of a product or service to its ongoing functioning.[265]

Finally, the CJEU functions as an important backstop to the deal making of any EU governmental body. As demonstrated by its *Schrems* decision, the CJEU is the ultimate interpreter of the requirements of EU data protection law.[266] Ireland has recently referred another important privacy case to the CJEU; this matter, universally termed *Schrems II*,[267] concerns the validity of both the standard contractual clauses and the Privacy Shield mechanism.[268]

B. Data Privacy Law in a Global Economy

This Section begins by discussing an overarching factor in the diffusion of EU privacy law, which is its creation of an easily transplantable regulatory model. It then concludes by considering three incidents from the history of data privacy law. The first occurred at the

---

262 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 189 (5th ed. 2019) (describing "California's Data Security Breach Notification Statute").

263 *Id.* at 152–57; *see* 15 U.S.C. § 6501(8), (9) (2012).

264 *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 1–2 (2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf; *see also* ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE 3 (2011), www.ontla.on.ca/library/repository/mon/25008/312239.pdf; *GDPR: Privacy by Design*, INTERSOFT CONSULTING, https://gdpr-info.eu/issues/privacy-by-design (last visited Mar. 7, 2019).

265 *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 179 (2018) ("When companies and lawmakers talk about privacy by design, they are often referring to procedures meant to ensure that privacy is a priority in organizational structure, organizational decision making, and the design of technologies."). The GDPR sets out its requirements for privacy by design in its Article 25 and discusses the concept generally in its Recital 78. *See* GDPR, *supra* note 29, art. 25, recital 78.

266 *See supra* Section II.B.2.b.

267 *See* Data Prot. Comm'r v. Facebook Ireland Ltd. [2017] IEHC 545 (H. Ct.) (Ir.), http://www.europeanrights.eu/public/sentenze/Irlanda-3ottobre2017-High_Court.pdf.

268 For an analysis of *Schrems II*, see Thomas Shaw, *The CJEU's 11 Key Questions in* Schrems II, IAPP (Apr. 16, 2018), https://iapp.org/news/a/the-11-key-considerations-in-schrems-ii-in-laymans-terms.

International Conference of Data Protection & Privacy Commissioners in October 1991 and offers a striking contrast to the next two incidents. The second of these events took place at the Privacy Shield Annual Review in October 2018, and the third at another conference of the commissioners, also held in October 2018. The contrast among these incidents serves to demonstrate not only a dramatic deepening of engagement between the United States and the EU around data privacy, but a victory for the EU in the marketplace of ideas about data privacy.

1. An Accessible Model

The GDPR and EU data protection principles have been applicable to legal systems and situations as diverse as Japan and the United States. Yet, the EU did not set out to become the world's privacy cop. Its power in this regard first developed in response to issues that it faced internally. It needed to harmonize the data processing practices of EU member states. The inward-facing elements of EU data protection law then became an important factor in its adaptability to the rest of the world. Here is a global diffusion story that begins with a response to internal political considerations.

As Weatherill notes, the EU's chief function is to manage the interdependence of its members.[269] In the realm of data protection, the EU proceeded by building on first-generation statutes dating back to the 1970's in France, Germany, Sweden, and a handful of other countries.[270] Abraham Newman summarized this initial process: "National legislation passed in the 1970s in several European countries was exported upward regionally . . . ."[271] Bradford generally and correctly notes that the EU did not set out to engage in "regulatory imperialism," but merely to express domestic policy preferences.[272] The EU's influence has been greatly extended, however, by its fortuitous development of a regulatory model for privacy that is comparatively easy to adopt outside the EU.

Omnibus privacy laws were the early choice for member states pioneering in data protection. Such laws regulate both the private and

---

269 WEATHERILL, *supra* note 186, at 396.

270 *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 21, 93, 165 (1989) (providing a comprehensive history and analysis of data privacy laws in various countries); J. Lee Riccardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?*, 6 B.C. INT'L & COMP. L. REV. 243, 247 n.29 (1983) (discussing Germany's promulgation of a comprehensive data privacy law following countries such as the United States and Sweden).

271 ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 3 (2008).

272 Bradford, *supra* note 47, at 6.

public sectors and do so through general rules for data collection and use. These statutes have also always been supplemented through sectoral laws that address specific areas. For example, German law has long provided sectoral privacy regulations in its telecommunications law, tax law, and commercial code.[273] Under the GDPR, member states are still permitted a range of sectoral regulations. Sometimes these regulations are necessary because an area falls outside the scope of the GDPR, such as national security matters.[274] Sometimes these more detailed regulations are permitted because the GDPR has left a question only partially resolved. For example, the GDPR sets sixteen years as the age at which a child may consent to the processing of personal data.[275] But the GDPR also allows member states to "provide by law for a lower age . . . provided that such lower age is not below 13 years."[276]

In contrast, the United States has favored information privacy statutes that regulate only individual sectors, such as credit reporting, video privacy, or financial institutions.[277] Unlike the EU, the United States lacks a general, safety-net omnibus regulation for personal information. In this regard, the Federal Privacy Act of 1974,[278] which sounds like it might be an omnibus privacy law, provides to be far less, regulating only data use by federal agencies.[279]

The use of omnibus laws in Europe proved a key element in the global diffusion of EU data protection law. Consider the Data Protection Directive of 1995, which consolidated existing national European laws and established a requirement that member states harmonize their data protection laws according to the Directive's standards.[280] With the fall of the Iron Curtain and the eastward expansion of the EU, each new member state was obliged to enact a harmonized national data protection law as part

---

273 *See* Abgabenordnung [Fiscal Code], § 87a; Handelsgesetzbuch [Commercial Code] § 257; Telekommunikationsgesetz [Telecommunications Act], § 89. The telecommunications law is now in the process of being amended. *See* Verkehrsdatenspeicherung, BUNDESNETZAGENTUR, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html (last visited Mar. 13, 2019).

274 *See* Consolidated Version of the Treaty on European Union, art. 4(2), Oct. 26, 2012, O.J. (C 326/1); GDPR, *supra* note 29, recital 16.

275 GDPR, *supra* note 29, art. 8(1).

276 *Id.*

277 *See* DANIEL SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 786–88 (6th ed. 2018) ("Consumer Privacy in the United States is regulated by 'sectoral' laws that focus on various sectors of the economy. Different laws regulate different industries.").

278 5 U.S.C. § 552a (2012).

279 Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 583 (1995).

280 *See* Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 85, at 1972.

of the price of joining the EU.[281] The general principles of the Directive and the harmonized EU data protection laws provided a relatively simple model first for the new member states of the EU and then for the rest of the world.

In 2001, Reidenberg had already noted the global trend to adopt EU-style data protection: "[T]he movement is also due, in part, to the conceptual appeal of a comprehensive set of data protection standards in an increasingly interconnected environment of offline and online data."[282] This conceptual appeal is matched by the accessibility of the EU model, anchored first in one Directive and then one Regulation, compared to the recondite and sprawling U.S. approach. Alan Watson has pointed to the degree of accessibility of a law as a main criterion for its potential success as a "legal transplant" when adopted by a foreign legal order.[283] In comparison to the sectoral-only U.S. approach, the simplified EU approach provides a highly attractive model for the rest of the world. The most recent proof of its success as a transplant comes from Brazil, which in August 2018 enacted the first Brazilian data protection law.[284] This statute is not only modeled on the GDPR but shares the same name: *Lei Geral de Proteção de Dados*.[285]

The replicability of the EU approach has been further demonstrated by the Safe Harbor and the Privacy Shield. These bilateral agreements have been mimicked by Switzerland, which has instituted similar agreements with the United States. In recent scholarship, Kristin Eichensehr envisions leading U.S. tech companies as large neutral entities, which she terms "Digital Switzerlands."[286] But this paradigm rests on an outmoded vision of Switzerland, which is itself not a "Digital Switzerland." In addition to its own Safe Harbor and then its own Privacy Shield with the United States,

---

281 See, for example, the discussion of a need for harmonized data protection in Latvia and Poland in the EU's "Comprehensive Monitoring Reports" before these countries joined the EU. EUROPEAN COMM'N, COMPREHENSIVE MONITORING REPORT ON LATVIA'S PREPARATIONS FOR MEMBERSHIP 17 (2003), https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/archives/pdf/key_documents/2003/cmr_lv_final_en.pdf; EUROPEAN COMM'N, COMPREHENSIVE MONITORING REPORT ON POLAND'S PREPARATIONS FOR MEMBERSHIP 19 (2003), https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/archives/pdf/key_documents/2003/cmr_pl_final_en.pdf.

282 Joel R. Reidenberg, *E-commerce and Transatlantic Privacy*, 38 HOUS. L. REV. 717, 737 (2001).

283 ALAN WATSON, LEGAL TRANSPLANTS: AN APPROACH TO COMPARATIVE LAW 94 (2d ed. 1993).

284 Lei No. 13.709, de 14 de Agosto de 2018, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 15.08.2018 (Braz.).

285 *See* Melanie Ramey, *Brazil's New General Data Privacy Law Follows GDPR Provisions*, INSIDE PRIVACY (Aug. 20, 2018), https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions.

286 Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665 (2019).

Switzerland has enacted an EU-style national data protection law and reached a coveted adequacy determination with the EU in 2000.[287] It is now undergoing the process of enacting a new, GDPR-friendly national data protection statute.[288] Its goal is to preserve its adequacy standing with the EU.[289] When it comes to personal data, even historically neutral Switzerland has closely aligned itself with the EU regarding the substance and process of data protection law.[290]

2. The Marketplace of Ideas

In October 1991 in Strasbourg, a law professor from the United States returned to the ongoing data protection commissioners' meeting, after taking a break, to be told that U.S. officials had just denounced him.[291] A U.S. State Department official charged that this academic had "misled" the world's data protection commissioner the previous year at their meeting in Paris.[292] The professor had reported that the United States only possessed "minimal privacy protections" and pointed out various shortcomings of American information privacy law, including its loopholes and poor level of oversight and enforcement.[293]

According to the leader of the U.S. delegation in 1991, the professor's speech did "not reflect U.S. policy nor . . . accurately reflect U.S. law."[294] The State Department representative told delegates and attendees that "the United States has considerable privacy protection, not omnibus, but nevertheless, considerable protection at both the federal and state level."[295] I was that professor, then teaching at the University of Arkansas (Fayetteville).[296] The previous year I had become the first American to address the world's data protection commissioners at their twelfth annual

---

287 *See* Commission Decision 2000/518/EC, of 26 July 2000 Pursuant to Commission Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided in Switzerland, 2000 O.J. (L 215) 1.

288 David Rosenthal, *Der Entwurf für ein neues Datenschutzgesetz* [The Draft of a New Data Protection Law], JUSLETTER (Nov. 27, 2017), https://media.homburger.ch/karmarun/image/upload/homburger/r1vRfY6_G-Jusletter_Beitrag_vom_27._November_2017.pdf.

289 *Id.*

290 On the essential influence of European data protection on the Swiss law in this area, see Rainer J. Schweizer, *Geschichte und Zukunft des Datenschutzrechts*, *in* DATENSCHUTZRECHT: BERATEN IN PRIVATWIRTSCHAFT UND ÖFFENTLICHER VERWALTUNG 9 (Nicolas Passadelis et al. eds., 2015).

291 *See* Evan Hendricks, *U.S. Official Blasts Law Professor's Description of Weak U.S. Privacy Law*, PRIVACY TIMES, Oct. 17, 1991, at 1.

292 *Id.*

293 *Id.* at 2.

294 *Id.*

295 *Id.*

296 *Id.* at 1.

meeting, held at the French Senate in Paris.[297] In response to the criticism from the U.S. government in Strasbourg, I asked for an opportunity to respond and made two points. First, that pursuant to the great American concept of the marketplace of ideas, the audience could decide whom to believe, and I certainly stood by my views on U.S. privacy law.[298] Second, that the criticism from the U.S. government represented "a very positive development."[299] It was positive as a leading indicator of potential future engagement with the global privacy debate.

It is worth quoting from my response at the 1991 commissioner's conference; by academic standards, it is a bit of a barn burner. More importantly, however, it serves as an indication of how much things have changed in terms of U.S. engagement in international data privacy law:

> Last year, in 1990, you had one American who was willing to speak to the Conference and that American was me. You didn't have any representative of the U.S. government who was willing to come to Paris and give a talk. Well, a year went by and we have three Americans here and . . . they are from the U.S. government. And what they're telling you is that everything is okay, and that I was misleading. Well, I think you see the direction we're moving in. If you ever give me a chance to speak again, you'll probably have six or seven Americans here . . . .
>
> But there's something else you can do. If you pass the . . . directive, . . . you'll have 15 Americans here. And I think at that point . . . they'll have concrete measures, and concrete examples as to how the United States is trying to improve its data protection laws . . . .[300]

The Data Protection Directive was passed in 1995, and its adequacy standard led in turn to the Safe Harbor and the Privacy Shield.[301]

Fast forward from that meeting in 1991 to October 2018, and the second annual review of the Privacy Shield. This meeting in Brussels featured not just six or seven Americans, but a substantial mix of more than one hundred American and European officials.[302] The delegation from the United States was not only numerous, but included such senior figures as the Secretary of Commerce and the Chairperson of the FTC, along with three of his key staff members, including the head of the agency's privacy enforcement division.[303] The U.S. delegation also contained

---

297 For my talk on that occasion in 1990, see Paul Schwartz, *American Data Protection Law Today*, *in* COLLECTION OF PAPERS: XIITH INTERNATIONAL CONFERENCE OF THE DATA PROTECTION COMMISSIONERS SEPTEMBER 17 18 19 1990, at 42 (1990).

298 Hendricks, *supra* note 291, at 2.

299 *Id.* at 3.

300 *Id.*

301 *See supra* Section II.B.2.

302 *EU, US Officials Meet for Second Privacy Shield Review*, IAPP (Oct. 18, 2018), https://iapp.org/news/a/eu-u-s-officials-meet-for-second-privacy-shield-review.

303 *See* Joseph Simons, Chairman, Fed. Trade Comm'n, Remarks at the Second Privacy

representatives from the Office of the Director of National Intelligence, the Department of Justice, and the State Department.[304] From that incident in 1991 to the Privacy Shield Review of 2018, there has been a dramatic increase in the level of engagement between the U.S. government and the EU around data privacy. There has also been an equally dramatic change in the conventional wisdom about the state of American information privacy law.

We now reach our third and final incident; it permits us to contrast that American professor's talk before the data protection commissioners in 1991 with a speech at the Forty-Second Meeting of the same group, held in Brussels on October 24, 2018. The speaker in 2018 was Tim Cook, the CEO of Apple, then the world's most valuable company.[305] This Article has already discussed Cook's conviction that privacy is a human right.[306] He offered that comment in May 2018 at the time of GDPR Day. By October of that same year, he went further and warned that personal data were being "weaponized" against the public.[307] Stockpiles of personal data were serving "only to enrich the companies that collect them."[308] Cook spoke out against how trade in personal information "has exploded into a data industrial complex" and praised the GDPR.[309] He flatly told the EU, "It is time for the rest of the world—including my home country—to follow your lead."[310] In concluding, Cook made it clear that he was speaking not only for himself, but for his company, and stated that Apple was "in full support of a comprehensive federal privacy law in the United States."[311]

Ideas matter. Even though the adequacy requirement provides an impressive fulcrum for international influence, the global success of EU data protection is also attributable to the sheer appeal of high standards for data protection. This appeal cannot alone be explained by the force of EU

Shield Annual Review (Oct. 18, 2018), https://www.ftc.gov/system/files/documents/public_statements/1416593/chairman_joe_simons_privacy_shield_review_remarks-2018.pdf.

304 Samuel Solton, *US Taking Privacy Shield Deal Seriously, EU Officials Say*, EURACTIV (Oct. 19, 2018), https://www.euractiv.com/section/data-protection/news/us-taking-privacy-shield-deal-seriously-eu-officials-say.

305 Tim Cook, CEO, Apple Inc., Remarks Before the International Conference of Data Protection & Privacy Commissioners (Oct. 24, 2018); *see* Noel Randewich, *Microsoft Overtakes Amazon as Second Most Valuable U.S. Company*, MSNBC (Oct. 26, 2018), https://www.reuters.com/article/us-usa-stocks-microsoft-amazon-com/microsoft-overtakes-amazon-as-second-most-valuable-u-s-company-idUSKCN1N02FQ (noting that Apple was the world's most valuable company at the time).

306 *See Apple CEO: Privacy Is Fundamental Human Right*, *supra* note 6.

307 Cook, *supra* note 305.

308 *Id.*

309 *Id.*

310 *Id.*

311 *Id.*

market power or even specific EU negotiating strategies. To illustrate, this Article can point to an example from the United States, namely, the enactment of the California Consumer Privacy Act (CCPA) of 2018.[312]

The CCPA began as a ballot initiative slated for the November 2018 election.[313] A series of high-profile international, national, and state privacy incidents made the passage of this proposition likely. In particular, the initiative sponsors pointed to the activities of Cambridge Analytica, a U.K. company. Cambridge Analytica had obtained data mined from millions of Facebook profiles to map personality traits with the goal of targeting ads and influencing the 2016 U.S. presidential election.[314]

The initiative's sponsors also demonstrated their political savvy by including a super-majority requirement for any amendment of it once enacted.[315] This made the initiative particularly threatening for tech companies because California's referendum process generally makes it difficult to amend a ballot initiative once enacted, and the 2018 privacy initiative would have created an even more stringent super-majority requirement for changing its terms.[316] In response, the business community in the Golden State negotiated a series of changes to the initiative with its sponsors, who agreed to drop it from the November ballot if the state legislature enacted the modified version.[317] The legislature in Sacramento quickly acted to pass a law embodying both the core principles of the initiative and the negotiated changes. On June 28, 2018, a single day before the deadline set by the initiative's sponsors, Governor Jerry Brown signed the law.[318] The CCPA goes into effect on January 1, 2020.[319]

The EU had not set up a policy shop in Sacramento, California. It had not lobbied the state legislature or Governor to enact a GDPR-like law. Yet, somehow, the ideas of EU data protection made their way to the

312 *See* California Consumer Privacy Act, A.B. 375 (Cal. 2018) (amended by S.B. 1121 (Cal. 2018)).

313 *See* John Myers & Jazmine Ulloa, *California Lawmakers Agree to New Consumer Privacy Rules that Would Avert Showdown on the November Ballot*, L.A. TIMES (June 21, 2018), https://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html.

314 *See, e.g.*, Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html ("It was suddenly easy to get people to sign the ballot petition [for the CCPA initiative]. 'After the Cambridge Analytica scandal, all we had to say was "data privacy,"' [Rick] Arney [cosponsor of CCPA initiative] [said].").

315 *Id.*

316 *Id.*

317 *See* Myers & Ulloa, *supra* note 313.

318 *California Consumer Protection Act (CCPA)*, OFFICE OF THE ATT'Y GEN., CAL., https://oag.ca.gov/privacy/ccpa (last visited July 6, 2019).

319 *See* Confessore, *supra* note 314.

Golden State. These include an individual's right to know what information a business has collected about them, a right to "opt out" of allowing a business to sell one's personal information to third parties, a right to deletion, a right to data portability, and a right to receive equal service and pricing from a business, even if one exercises her rights under the Act.[320]

Different policy concepts and, more specifically, regulatory approaches compete against each other in a marketplace of ideas. Agreements such as the Safe Harbor and Privacy Shield have provided an important focal point for the acculturation of lawyers, consultants, and policymakers in the United States. In entering the Safe Harbor or Privacy Shield, for example, organizations receive a crash course in EU data protection law. The result has been widespread familiarity with EU-style data protection and, over time, buy-in to its ideals. This phenomenon represents another way the EU has not singlehandedly imposed its regime on nations, but rather reached important actors through the force of appealing ideas and a range of different kinds of interactions, which lead to a general process of acculturation to EU privacy concepts.

CONCLUSION

GDPR Day gave the impression of a momentous, global shift established by a single actor—the EU—through a single law—the GDPR. Analogously, Bradford, as well as Goldstein and Wu, view the EU as a de facto unilateral power that other nations and private companies have scant choice but to follow. Their scholarship bases this perspective on the EU's significant market power, the difficulties inherent in creating different products and services for EU citizens and non-EU citizens, and the EU's regulatory capacity. But this Article has shown that the diffusion of EU data protection does not neatly fit this model.

The EU has undeniable regulatory capacity, as well as influence over the private and public sectors in other countries. The way it has achieved a global stature for its data protection law, however, is telling of the nature of its power: it has been neither unilateral nor purely de facto, and the EU's influence cannot be solely attributed to economic forces. This Article's case studies on Japan and the United States reveal three lessons in this regard. First, rather than exercising unilateral power, the EU engages in bilateral negotiations. Second, the adequacy requirement provides significant leverage in these negotiations, which the EU uses with flexibility to reach good faith adequacy agreements now while requiring bilateral reviews later as a check on foreign jurisdictions. As for the third

320 *See Corporate Alert: California Passes Landmark Consumer Privacy Act—What It Means for Business*, AKIN GUMP, LLP (July 9, 2018), https://www.akingump.com/en/news-insights/california-passes-landmark-consumer-privacy-act-what-it-means.html.

lesson, the EU's regulatory capacity reflects a complex interplay among its institutions, as well as adoption of outside influences. Bradford insightfully points to the general importance of the EU's expertise, which is certainly present in the field of data privacy. Yet, this capacity is further enhanced by a dispersal of power within the EU and its multiplicity of policy and lawmaking institutions, each buttressing one another in maintaining high standards for data privacy.

Finally, the diffusion of EU data protection law has been promoted by two additional factors. First, some legal approaches are better candidates for transplantation than others. Accessible legal models like omnibus data privacy laws are adopted in part due to their ease of enactment and comprehensiveness. Just as the EU saw value in omnibus laws in the 1970s, other nations have recognized the merits of this approach. Second, as shown by California's CCPA, EU-style data protection has proven to be an appealing idea that a large number of jurisdictions have adopted. The global diffusion of EU data protection reflects a success in the marketplace of ideas.