Forthcoming 94 NYU Law Review -- (2019)

Global Data Privacy: The EU Way

By 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.

---

* Jefferson E. Peyser Professor of Law at UC Berkeley School of Law; Director, Berkeley Center for Law & Technology.

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, there was a consensus that it represented a law not only for the EU, but for the world. 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.[2] Indeed, 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 "U.S. companies have already invested billions of dollars to comply with the new rules" of this law.[3]

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."[4] In a similar fashion, Tim Cook, the CEO of Apple, told CNN that "privacy is a fundamental human right."[5] The description of privacy through rights-talk is a core aspect of the EU approach to data privacy. The U.S. legal system views information privacy as a consumer interest, but data protection in the EU is seen as a fundamental right, and one that rests on interests in dignity, personality, and informational self-determination.[6]

The question then becomes *why* the world follows the EU's lead in this area. Data privacy law is one of the most important areas of data 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. Contrary to the one-fell-swoop perception of EU influence evoked by GDPR Day, there has, in fact, been a varied range of nation-

---

[1] Quentin Aries, Tommy Romm & James McAuley, 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.

[2] Helen Dixon, Regulate to Liberate: Can Europe Save the Internet?, Foreign Affairs (Sep./Oct. Issue), 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 GPDR notes.").

[3] 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.

[4] Brad Smith (@BradSmi), Twitter (May 21, 2018, 1:40PM), https://twitter.com/BradSmi/status/998664978063241216.

[5] Apple CEO: Privacy Is a Fundamental Human Right, CNN (Jun. 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).

[6] For a discussion, see Paul M. Schwartz & Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, 106 Geo. L.J. 115, 123–27 (2017).

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 kind of unilateral power. In particular, Bradford's model portrays a powerful "Brussels Effect" that largely rests on the EU's "de facto unilateral" influence. 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. Armed with a concomitant data embargo power, the EU has engaged in separate adequacy negotiations with Japan, the U.S., and other countries. In Japan, these negotiations have taken the form of an application for a determination of adequacy from the EU Commission. The U.S., 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.

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 (CJEU) 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.

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. As a second 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. 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.

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." 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 unanimous 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

Widespread media coverage, conferences, speeches, and the tweeting of memes marked GDPR Day.[7] The numerous memes devoted to the GDPR drew on popular culture, including Jules from *Pulp Fiction* brandishing a gun ("Say GDPR One More Time"),[8] and a parody of the initial screen crawl from *Star Wars* ("We have updated our GLOBAL PRIVACY TERMS. Your trust is important to us" followed by additional, likely endless boilerplate).[9] A leading vendor in privacy compliance technology, TrustArc handed out "GDPR Recovery Kits" at industry conferences. These were small nylon zipper bags containing aspirin, vitamin C, and similar hangover remedies.

Substantively, observers of GDPR Day emphasized the high sanctions and aggressive enforcement available under the regulation. For example, the GDPR permits fines up to 4% of a company's worldwide revenue or 20 million Euros, whichever is greater.[10] 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

---

[7] Angela Wattercutter, How Europe's GDPR Regulations Became a Meme, Wired (May 25, 2018), https://www.wired.com/story/gdpr-memes//.

[8] Cardens Accountants (@CountOnCardens), Twitter (May 18, 2018, 2:37AM), https://twitter.com/CountOnCardens/status/997410776389439489.

[9] Rian Johnson (@rianjohnson), Twitter (May 24, 2018, 12:15PM), https://twitter.com/rianjohnson/status/999730569641525248.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 83–84, 2016 O.J. (L. 119) 1 (EU) [hereinafter GDPR].

his or her behalf."[11] 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." These NGOs were said to be placing tech companies under "new legal siege."[12] 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.'"[13]

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."[14] 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.[15] 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.[16] Greenleaf noted that at least thirty more countries had official bills for such laws.[17] In his assessment, "Something reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws."[18]

Furthermore, principles found in the GDPR, such as data portability and the "right to be forgotten," are already influencing laws outside Europe. 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."[19] 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

---

[11] *Id.* at art. 80.

[12] Quentin Aries, Tommy Romm & James McAuley, 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.

[13] 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 (published in print with the headline: "Newly Armed, Irish Regulator Takes on Tech").

[14] Jan Philipp Albrecht & Florian Jotzo, Das Neue Datenschutzrecht der EU 126–29 (2017).

[15] Business Groups Call for Leniency Ahead of GDPR Entry into Force, Parliament Magazine (May 18, 2018), https://www.theparliamentmagazine.eu/articles/news/business-groups-call-leniency-ahead-gdpr-entry-force.

[16] Graham Greenleaf, Global Data Privacy Laws 2017, 145 Privacy Laws & Business Int'l Report, 10–13.

[17] *Id.*

[18] Graham Greenleaf, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, 2 Int'l Data Privacy Law 2, 13 (Oct. 2011).

[19] 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)), UNSW Law Research Paper No. 18-56 (May 25, 2018), available at https://ssrn.com/abstract=3184548.

plans for its enactment and debates about its content had begun long before.[20] 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 from different jurisdictions. The leading accounts of the worldwide diffusion of EU privacy law have come to similar conclusions about the EU's singular power. This Article first examines the influential work of Jack Goldsmith and Tim Wu on this issue, then turns to the valuable scholarship of Anu Bradford.

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 market power and its unusual concern for its citizen's privacy."[21] 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."[22] Furthermore, under many circumstances, international companies cannot geographically screen their EU customers and, even if they could, do not wish to create separate services for them.[23] 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. The result, according to Goldsmith and Wu, is that U.S. companies have chosen to bow to the "significant market power" of the EU.[24]

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.[25] Beyond privacy, Bradford examines a number of areas, including antitrust, consumer protection, and environmental protection. As she points out, EU regulations have "a tangible impact on the everyday lives of citizens across the world."[26] 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

---

[20] European Data Protection Supervisor (EDPS), The History of the General Data Protection Regulation (2018), https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[21] Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World 176 (2006).

[22] *Id.* at 175.

[23] *Id.*

[24] *Id.* at 176.

[25] Anu Bradford, The Brussels Effect, 107 Nw. U.L. Rev. 1 (2015), https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1/.

[26] *Id.* at 3.

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."[27]

Where Goldsmith and Wu see unilateral power in the EU's privacy law, Bradford further specifies that the Brussels Effect is one of "de facto unilateral regulatory globalization."[28] 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."[29] 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.[30] 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."[31]

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.[32] Here, there can be a "de jure Brussels Effect," but Bradford conceives of it as following a set timeline. As Bradford writes, "Corporations' de facto adjustment to the EU rules paves the way for legislators' de jure implementation of these rules."[33]

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)."[34] A final essential factor concerns whether a firm's conduct or production is "nondivisible," meaning it would not be feasible to have different standards for different markets.[35] As Bradford explains, the inability to set up different compliance standards—whether for legal, technical or economic reasons—creates a powerful condition "for a jurisdiction to dictate rules for global commerce."[36]

Under Bradford's factors, there is indeed much evidence that would predict 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.

---

27 *Id.*
28 *Id.* at 38.
29 *Id.*
30 *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.").
31 *Id.* at 6.
32 *Id.*
33 *Id.* at 8.
34 *Id.* at 5.
35 *Id.*
36 *Id.*

Goldsmith and Wu rightly emphasize this point.[37] The EU represents the second largest economy in the world, and the second largest consumer market in the world.[38] More specifically, the EU has been an early adopter of a wide range of information technology and has been at the top or close to it in critical areas such as broadband internet connections. International tech giants have moved quickly to offer their products and services in the EU, which has been an important source for these entities' gathering of personal data. As just one example, Facebook has more users in Europe (17% of its world users) than in North America (13%).[39]

Second, the EU has built up considerable regulatory capacity for privacy. At the Member State level, each country has a Data Protection Authority.[40] Within the EU, data protection has long been a focus of directorate generals (DGs). DGs are part of the European Commission, the executive arm of the EU, and each one is devoted to a specific field or fields of expertise.[41] The Parliament also demonstrates strong interest in this topic, with the LIBE Committee currently playing a central role within that institution.[42] Finally, there are important independent EU privacy entities, including the European Data Protection Supervisor[43] and, under the GDPR, the European Data Protection Board.[44]

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 absolute, quantifiable certainty of the risk."[45] As for the elasticity of personal data markets, Bradford finds that companies may face difficulties in isolating services exclusively for EU operations.[46] Here, too,

---

[37] Goldsmith & Wu, *supra* note 21, at 175.

[38] Bradford, *supra* note 25, at 11–12. In 2017, China led the world with a GDP of $23.16 trillion, followed by the EU ($20.85 trillion) and the U.S. ($19.39 trillion). Central Intelligence Agency, CIA World Factbook, https://www.cia.gov/library/publications/the-world-factbook/. 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.*

[39] Facebook Users in the World, Internet World Stats (Jun. 30, 2017), https://www.internetworldstats.com/facebook.htm.

[40] National Data Protection Authorities, Eur. Comm'n (Sep. 21, 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

[41] How the Commission Is Organised, Eur. Comm'n, https://ec.europa.eu/info/about-european-commission/organisational-structure/how-commission-organised_en.

[42] The Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) has played a key role in developing the GDPR, investigating the Facebook Cambridge-Analytica breach, updating the ePrivacy Regulation, and reviewing the EU-U.S. Privacy Shield. LIBE Committee, Electronic Privacy Information Center, https://epic.org/privacy/intl/LIBE/default.html (last visited, Oct. 22, 2018).

[43] The first EDPS was appointed in 2004. Decision 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 2004/55/EC (European Data Protection Supervisor), 2004 O.J. (L. 12) 47.

[44] GDPR, *supra* note 10, art. 68.

[45] Bradford, *supra* note 25, at 15.

[46] *Id.* at 25 ("Data flows lightly and instantly across borders . . . At times, it is technologically difficult or impossible to separate data involving European and non-European citizens.").

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. A contrast should be drawn with labor markets, where companies may be more easily able to isolate employment practices country-by-country.[47] As Bradford observes, labor markets are easily divisible, but data services are not. 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."[48] Overall, according to Bradford, personal data appears to fulfill the conditions for a de facto unilateral Brussels Effect.[49]

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. In the second, the U.S. went outside of the formal adequacy process and negotiated opt-in agreements for U.S. companies that wish to comply with EU standards. 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 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

EU law has long contained both a threshold test for international transfers of personal data to countries outside its territory and a legal basis for blocking data exports to nations that do not meet this standard. The logic of EU policymakers here is impeccable. As a technological matter, digital data can be transmitted throughout the world in a largely friction-free exercise.

---

47 *Id.* 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.").

48 *Id.* at 17.

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

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. 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."[50] This approach is necessary to prevent the creation of privacy-free data oases outside the reach of EU data protection.

The standard for these extraterritorial transmissions has long been that of "adequacy" of data protection in the foreign jurisdiction. In 1995, the Directive on Data Protection, the precursor to the GDPR, established an adequacy requirement for international data transmissions.[51] In 2016, the GDPR maintained this same requirement and strengthened the process around it.[52] Under both the Directive and the GDPR, adequacy can be met by the country's law as a whole, by a sub-territory within a country, or by the terms of the specific transfer.[53] Along 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.[54]

There is a pre-history to the adequacy requirement, which reveals it to be a compromise solution. Prior to the Directive, many EU nations required "equivalent" protections in another country before allowing transfers of personal data outside of their territory.[55] The Directive took this "equivalency" standard and limited it to members of the EU.[56] Under the Directive, Member States were obliged to enact harmonizing legislation and subsequently to permit transfers *inside* the EU without any further formalities.[57] In this fashion, the Directive helped create a single market for personal data in the EU—and 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.

---

[50] Paul M. Schwartz, The EU-US Privacy Collision: A Turn to Institutions and Procedures, 126 Harv. L. Rev. 1966, 1984 (2013); *see generally* Paul M. Schwartz, European Data Protection Law and Restrictions on International Data Flows, 80 Iowa L. Rev. 471 (1994).

[51] 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 Data Protection Directive].

[52] GDPR, *supra* note 10, arts. 44–50.

[53] *See id*., arts. 45–47; s*ee also* Julian Wagner, The Transfer of Personal Data to Third Countries Under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?, International Data Privacy Law (Jul. 2, 2018), https://doi.org/10.1093/idpl/ipy008 ("In the absence of such an adequacy decision, an export is . . . only allowed if additional safeguards are provided, such as BCR [binding corporate rules] and standard data protection clauses adopted by the EC [European Commission].").

[54] Data Protection Directive, *supra* note 51, art. 25(4); GDPR, *supra* note 10, art. 44.

[55] Schwartz, European Data Protection Law and Restrictions on International Data Flows, *supra* note 50, at 474–77 (summarizing the requirements of several European countries in 1995 and finding an emerging consensus around the equivalency standard).

[56] Data Protection Directive, *supra* note 51, Recital 8, at 32.

[57] Schwartz, The EU-US Privacy Collision: A Turn to Institutions and Procedures, *supra* note 50 at 1973–74.

The Directive stated that international transfers were to be permitted "only if . . . the third country in question ensures an adequate level of protection."[58] 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."[59] The Directive also contained six exceptions to its adequacy requirement for international transfers, including one where the "data subject" consented to the transmission.[60] Finally, the Directive called for the Commission to maintain "white lists" of countries with adequate data protection.[61] There are now eleven countries on this list, which means entities in the EU can transfer data to these nations without any further requirements.[62] A transmission to a nation on the white list 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 in the Member States. Similar to the Data Protection 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 sector, . . . as well as the implementation of such legislation, data protection rules, professional rules and security measures."[63]

Rules for the EU's internal procedures for finding adequacy have changed over the years. 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.[64]

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 U.S. concerning the adequacy requirement. These case studies, however, reveal more complexity than fits within the de facto unilateral model of EU privacy law diffusion.

---

58 Data Protection Directive, *supra* note 51, art. 25(1).

59 *Id.* at art. 25(5).

60 *Id.* at art. 26.

61 Data Protection Directive, *supra* note 51, art. 30(6).

62 Adequacy of the Protection of Personal Data in Non-EU Countries, Eur. Comm'n, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

63 GDPR, *supra* note 10, art. 45(2)(a).

64 European Commission Press Release IP/18/5433, International Data Flows: Commission Launches the Adoption of Its Adequacy Decision on Japan (Sep. 5, 2018), http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

B. Different National Approaches

This Section examines the paths taken to reach adequacy in Japan and the U.S. The situation in each country was different, and the EU demonstrated considerable flexibility in response to these varying political and economic landscapes.

1. Japan: Adequate National Law

On July 17, 2017, the EU and Japan concluded negotiations toward an EU finding of adequate data protection in Japan.[65] The EU has now released a draft Commission Implementing Decision[66] and started its internal process of formal approval of an adequacy finding.[67] At a G7 summit in 2017, the Prime Minister of Japan, Shinzo Abe, and the President of the European Commission, Jean-Claude Juncker, welcomed this progress. They pointed to the convergence between the EU and Japanese systems and a shared approach resting "on an overarching privacy law, a core set of individual rights and enforcement by independent supervisory authorities."[68] The Japanese-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.[69]

Japan now stands on the threshold of entry onto the EU's coveted "white list" of adequate nations.[70] This development is a surprising one. In his 2014 overview of Asian privacy law, Greenleaf titled his chapter on Japan, "The Illusion of Protection."[71] 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." Greenleaf also noted an absence of evidence showing that Japan enforced its data protection law.[72] Rather than an enforceable system for privacy protection, Greenleaf

---

65 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), http://europa.eu/rapid/press-release_IP-18-4501_en.htm.

66 European Commission, Draft Adequacy Decision – Commission Implementing Decision Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan [*hereinafter* EU Implementing Decision on Japan Adequacy].

67 European Commission Press Release IP/18/5433, *supra* note 64.

68 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), europa.eu/rapid/press-release_STATEMENT-17-1917_en.pdf.

69 GDPR, *supra* note 10, art. 45(2).

70 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/.

71 Graham Greenleaf, Asian Data Privacy Laws 227 (2014).

72 *Id.* at 263.

characterized Japanese law as a set of "ritual observances, with little evidence of tangible results."[73]

How did the Japanese go from having an illusory system of data privacy in 2014 to one that the EU Commission is willing to place on its 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).[74] 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).[75]

As another novel dimension, the amended APPI contains protection for international transfers of personal data from Japan. In taking this step, Japan adopted a prominent idea of EU data protection law. The 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 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.[76]

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-Japanese engagement in reaching the adequacy determination. The ensuing changes to Japanese law begin with a set of so-called "Supplementary Rules" issued by the Japanese data protection commission, which have the full effect of legislatively-enacted law.[77] Some of the ensuing protections are limited only to EU-originated personal data.[78] For example, a supplementary protection extends the APPI's list of "sensitive data" to "data transferred from the European Union concerning an individual's sex life, sexual orientation or trade-union membership."[79] This change to Japanese data

---

[73] *Id.* at 562.

[74] Personal Information Protection Commission, Japan, Amended Act on the Protection of Personal Information ver. 2 (Dec. 2016), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

[75] Michihiro Nishi, Japan: Data Protection in Japan to Align with GDPR, Mondaq (Sep. 27, 2018), http://www.mondaq.com/x/739986/Data+Protection+Privacy/Data+Protection+In+Japan+To+Align+With+GDPR.

[76] Personal Information Protection Commission, Japan, Amended Act on the Protection of Personal Information ver. 2 (Dec. 2016), *supra* note 74, at Art. 24.

[77] European Commission, Supplementary Rules Under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU Based on an Adequacy Decision (Annex I), https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf; Michihiro Nishi, *supra* note 75.

[78] *Id.* at ¶31.

[79] *Id.* at ¶68.

protection extends protections for "special care-required personal information" to the categories recognized as "sensitive data" in the GDPR, Article 9(1).[80] This coverage is only for personal data from the EU, however, and not for Japanese personal data processed in Japan.

In addition to the Supplementary Rules, the EU-Japanese 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."[81] The Annex also details how oversight of data protection is to be carried out in Japan's public sector.[82]

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.[83] It requires scrutiny of "all aspects of the functioning" of the Decision with particular attention paid to the application of the Supplementary Rules and to how Japan protects its onward transfers to non-EU countries.[84]

Finally, in an innovative step, the proposed EU-Japan adequacy finding will run in two directions. The two parties will make a finding of "reciprocal adequacy."[85] Until this moment, all the EU's findings of adequacy for a nation's data protection concerned the status only of the non-EU country.[86] The EU's findings of adequacy for Argentina, Canada, Israel, New Zealand, or any other so-called "third country," concerned only the flow of personal data from the EU to that non-EU entity.[87] In contrast, the EU and Japan have crafted an adequacy decision that recognizes each other's data protection systems.[88] 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. To further this goal, Japan has created a data embargo power for its national privacy authority.

Mutual reciprocity demonstrates the diffusion of EU ideas. It also illustrates the linkage between economic considerations and data protection.

---

80 *See* GDPR, *supra* note 10, art. 9(1).

81 Collection and Use of Personal Information by Japanese Public Authorities for Criminal Law Enforcement and National Security Purposes (Annex II), Personal Information Protection Commission, Japan (Sep. 14, 2018) at 23, https://ec.europa.eu/info/sites/info/files/annex_ii_signed_representation_en.pdf.

82 *Id.* at 23.

83 EU Implementing Decision on Japan Adequacy, *supra* note 66, at ¶181.

84 *Id.*

85 *Id.*

86 Hunton Andrews Kurth LLP, EU and Japan Agree on Reciprocal Adequacy (July 17, 2018), https://www.huntonprivacyblog.com/2018/07/17/eu-japan-agree-reciprocal-adequacy/.

87 *Id.*

88 European Commission Press Release IP/18/4501, *supra* note 65.

This Article has spoken of GDPR Day, May 25, 2018, as a historical occasion.[89] But an earlier milestone was reached on July 17, 2017. On that day in Tokyo and Brussels, the EU and Japanese government announced both the adequacy decision and their equally ambitious economic partnership agreement.[90] The EU-Japan Economic Partnership Agreement removes a wide range of trade barriers between the two jurisdictions.[91] It is the largest trade deal negotiated by the EU and will create an open trade zone with over 600 million people in it.[92] In a press release issued from Tokyo, the European 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 for personal data."[93] Emphasizing the economic benefits of this arrangement, Vera Jourová, EU Commissioner for Justice, 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."[94] 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. The point could not be clearer: data protection is good for international business.

2. The U.S. and the Privacy Shield: Private Sector Opt-in

The U.S. has never formally sought an adequacy determination from the Commission. According to Christopher Wolf, the American reluctance follows from the "well-understood outcome" of such a request: "request denied."[95] Instead, the U.S. and EU have settled on a strategy around à la carte findings of adequacy. Before the Safe Harbor and independent of its negotiations with the U.S., the EU had already developed two such paths: standard contractual clauses[96] and Binding Corporate Rules (BCRs).[97] The standard contractual clauses establish approved rules for transmitted data. If used, these clauses must be signed for each transfer by the sending entities in the EU and the receiving entities in the U.S.[98] The BCRs are internal corporate rules for data transfers

---

89 *See supra* Part I.A.

90 EU and Japan Sign Economic Partnership Agreement, Eur. Comm'n (July 17, 2018), http://trade.ec.europa.eu/doclib/press/index.cfm?id=1891.

91 European Commission Memo, Key Elements of the EU-Japan Economic Partnership Agreement (July 6, 2017), http://trade.ec.europa.eu/doclib/press/index.cfm?id=1687.

92 EU and Japan Sign Economic Partnership Agreement, *supra* note 90.

93 European Commission Press Release IP/18/4501, *supra* note 65.

94 *Id.*

95 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. & Po'y 227, 229 (2013).

96 European Commission Decision 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, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en.

97 Binding Corporate Rules, Eur. Comm'n, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en.

98 Standard Contractual Clauses, *supra* note 96.

within multinational organizations.[99] The EU describes them as being "like a code of conduct" to cover a company's data practices worldwide.[100]

Standard contractual clauses and BCRs are open to any entities in a country not on the "white list" of adequate nations. 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 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."[101] 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 U.S.

More broadly than these measures, the EU and U.S. have developed two programs of voluntary private sector compliance. These are, first, the Safe Harbor[102] (2000 to 2015), and then, the Privacy Shield[103] (2016 to present). In these two bilateral agreements, the EU and U.S. 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 present a streamlined list of substantive EU principles for American companies to follow voluntarily. This Section now focuses on the Safe Harbor and the Privacy Shield. It also considers the key role played by the CJEU through its *Schrems* decision.

The Safe Harbor. Faced with the EU's view that the U.S. does not provide adequate data protection, the U.S. engaged in discussions with it regarding a possible solution to allow international data flows to continue from the EU to the U.S. In 2000, following multi-year bilateral negotiations, the Commission of the EU and the U.S. Department of Commerce agreed on the Safe Harbor Agreement. In the resulting document, there was something for both sides.

---

99 Binding Corporate Rules, *supra* note 97.

100 *Id.*

101 GDPR, *supra* note 10, art. 45(1).

102 Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000); 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); Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7.

103 Department of Commerce, EU-U.S. Privacy Shield, Washington, DC, February 29, 2016, https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

The U.S. government did not have the votes in Congress to enact an omnibus, EU-style privacy law. Indeed, leading U.S. tech companies of that era were strongly opposed to such a law. By allowing U.S. companies to voluntarily accept the Safe Harbor principles, however, the U.S. government found a way to permit data transfers to continue to the U.S. 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 the personal data of EU residents.

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. Thus, 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.[104] 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.

On the EU-side, negotiators recognized the political realities in the U.S. and the unlikelihood of enactment of an omnibus U.S. privacy statute. 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. 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."[105]

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 generally observes, "Trade is the EU's business."[106] 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. The EU has therefore sought to promote not only data protection, but the free flow of data. As the Data Protection Directive stated, "cross-border flows of personal data are necessary to the expansion of international trade."[107] Achieving this goal means finding a way to facilitate trade with the U.S., the EU's most important external trade partner.

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)

---

[104] Henry Farrell, Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement, 57-2 Int'l Org. 277, 291 (2013).

[105] Testimony of Joel R. Reidenberg, Prof. of Law, Hearing on the EU Data Protection Directive: Implications for the U.S. Privacy Debate, U.S. House of Reps., Mar. 8, 2001, http://reidenberg.home.sprynet.com/Reidenberg_Testimony_03-08-01.htm.

[106] Stephen Weatherill, Law and Values in the European Union 407 (2016).

[107] Data Protection Directive, *supra* note 51, Recital 56.

security; (5) data integrity; (6) access; and (7) enforcement.[108] 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. By 2015, some 4,500 U.S. companies had publicly affirmed their following of the Safe Harbor and listed their names on the official site for the agreement, which the U.S. Commerce Department maintained.[109]

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 U.S. 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.

On the EU-side, however, controversy accompanied the Commission's judgment that the Safe Harbor met the adequacy standard. In 2000, the EU Parliament passed a non-binding resolution rejecting the Safe Harbor. In prescient testimony to the U.S. Congress in 2001, moreover, Reidenberg predicted that the Safe Harbor was vulnerable to collapse.[110] 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.[111]

The Demise of the Safe Harbor and Birth of the Privacy Shield. In 2015, the U.S. and the EU were well underway in negotiations for modifications to the Safe Harbor. A decision of the 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.[112] This result strengthened the hand of the EU in its high-stake negotiations with the U.S. The decision also constitutionalized important aspects of data protection law.

In *Schrems*, the Luxembourg Court found that the Safe Harbor fell short of the requirements of the Data Protection Directive, as read in light of the European Charter.[113] 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

---

[108] Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks, Fed. Trade Comm'n (Dec. 2012), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

[109] Martin A. Weiss & Kristin Archick, Cong. Research Serv, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield (2016), https://fas.org/sgp/crs/misc/R44257.pdf.

[110] Testimony of Joel R. Reidenberg, *supra* note 105.

[111] *Id.*

[112] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 ¶ 73, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362 [https://perma.cc/G4YP-33Z2].

[113] *Id.*

principles of the transnational agreement.[114] Moreover, the EU High Court faulted the Safe Harbor for "permitting the public authorities to have access on a generalised basis to the content of electronic communications."[115] Such an approach "must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[116]

This decision also settled questions regarding the meaning of the adequacy standard established by the 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.[117] 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. In these and other detailed comments in its *Schrems* decision, the Luxembourg Court provided a roadmap for EU negotiators by making clear its expectations for any future agreement with the U.S post-*Schrems*.

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. In recognition of the ongoing transatlantic negotiations, however, European data protection authorities agreed not to prosecute companies who continued to use the Safe Harbor agreement post-*Schrems*. By early 2016, negotiations between the EU and U.S. for a successor agreement proved successful, and the EU and U.S. Department of Commerce released the details of the Privacy Shield. Following demands from the EU Parliament in March 2016, the Department of Commerce strengthened some aspects of the agreement and received final approval from the Parliament in July 2016. The official implementation of the Privacy Shield began on August 1, 2016.

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. The considerable overlap between the Privacy Shield and Safe Harbor Principles means a continuity in basic vocabulary and orientation, which potentially offers 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 the Safe

---

114 *Id.* at ¶ 86.
115 *Id.* at ¶ 94.
116 *Id.* at ¶ 94.
117 *Id.* at ¶ 73–74, 96.

Harbor's principle of "Enforcement."[118] It reconfigures this concept as "Recourse, Enforcement, and Liability."[119] 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 Principles referred by EU Member State authorities through the Department" as well as other aspects of the enforcement process.[120] 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."[121] 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 to safeguard against individuals being pressured to make choices to their detriment.

Beyond these changes to the Safe Harbor Principles, new institutional commitments by the U.S. 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.[122] These assurances are important in light of the CJEU's concerns in *Schrems* about the U.S. engaging in supposedly indiscriminate mass surveillance of EU data. Moreover, the Commission's implementing decision of July 12, 2016 emphasized the requirement of periodic reviews of its adequacy finding.[123] Looking to the future, many elements of the current framework 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 idea that the EU exercises unilateral power and reaches only de facto results. Instead, they demonstrate that the EU has employed 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.

---

118 Commission Decision, *supra* note 102.

119 Department of Commerce, EU-U.S. Privacy Shield, Washington, DC, Annex I, EU-U.S. Privacy Shield Principles 6, February 29, 2016, https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

120 *See id.* at 7.

121 *Id.*

122 Letter from Robert S. Litt, General 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. (Feb. 22, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F.

123 European Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

A. Lessons from the Case Studies

In Japan, the process of reaching an adequacy agreement proved to be neither unilateral nor de facto. Unlike a unilateral imposition, Japan chose to engage in bilateral negotiations with the EU and create a reciprocal agreement that results in the world's largest zone for free data exchanges. Furthermore, the result is de jure, not de facto law.[124] The commitments were carefully documented in both Japan's data protection law and the Supplementary Rules and Annexes to the Commission Implementing Decision.[125] 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. Rather, Japan's choice of a system similar to and compatible with EU data protection law has been a qualitative one. Behind it is not only Japan's assessment of its economic interests, but also a judgment regarding the merits of competing data privacy regulatory systems. Just as Japan adopted Germany's civil code in 1896, it chose to follow the path of EU law in this century and modified Japanese law accordingly.[126]

Regarding the U.S., the EU proved open to bilateral dealmaking in its negotiations around the Safe Harbor and the Privacy Shield. The Safe Harbor and the Privacy Shield modified classic EU principles just enough to make the results tolerable on the American-side of the Atlantic, while being defensible in Brussels and within Member States. Rather than a unilateral exertion of power, these negotiations show striking flexibility and cooperation on the EU's part.

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. 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. U.S. companies had not lobbied for it, and the idea itself came from Ambassador David Aaron, the critical 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.[127]

This approach has also been a great success with the U.S. private sector.[128] 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

---

[124] *See supra* Part II.B.1.

[125] EU Implementing Decision on Japan Adequacy, *supra* note 66; Annex I, *supra* note 77, Annex II, supra note 81.

[126] Zentaro Kitagawa, Development of Comparative Law in East Asia, in Oxford Handbook of Comparative Law 236, 239-42 (M. Reimann & R. Zimmermann, eds. 2006).

[127] Farrell, supra note 104, at 292.

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

participants as it took the Safe Harbor 13 years to achieve."[129] The EU strategy has reaped significant rewards; it has effectively changed the data privacy practices of many organizations in the U.S. for processing EU data and even non-EU data. The EU has worked with regulators, and also reached around regulators in the U.S. 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.

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-US Safe Harbor. 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?"[130] 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.

The case study of Japan also demonstrates that, over time, the EU has been able to learn from past negotiations and, in general, to heighten the bar for meeting its adequacy test. In 2003, the Commission found Argentina to have adequate data protection in a brief four-page decision.[131] To some observers, this action was proof of the arbitrary nature of the EU's "white list" for data transfers. 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 alone the world. In 2017, the Commission acknowledged its use of this general criteria, at least for the purpose of deciding whether to pursue "a dialogue on adequacy."[132] In starting such a conversation, 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."[133]

Japan certainly has a pioneering potential for other Asian countries deciding on a privacy regime, but it nevertheless faces a more complicated and,

---

[129] *Id.*

[130] Graham Greenleaf, Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles, 154 Privacy Laws & Bus. Int'l Report 1, 10 (2018), http://www.austlii.edu.au/au/journals/UNSWLRS/2018/53.html.

[131] 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, 2003 O.J. (L 168) 19.

[132] 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), http://europa.eu/rapid/press-release_MEMO-17-15_en.htm.

[133] *Id.*

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.[134] 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. Korea is now in the process of negotiations to join the EU's "white list" as well.[135]

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 U.S. respectively.

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.[136] 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 dispersal of power within the EU legislative process—a dispersal that allows [fundamental rights] consideration ignored by some institutions to be brought to light by others."[137] To illustrate, the data protection authorities in the Member States have an essential role under the GDPR.[138] These officials must approve companies' use of BCRs to ensure that all data transfers within a corporate group meet EU standards.[139] The European Data Protection Supervisor (EDPS) and the European Data Protection Board additionally are granted important roles by the GDPR.

As part of this institutional interplay, the EU has been open to ideas 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 2000 and now found in all fifty American states.[140] From the federal U.S. Children's Online Privacy Protection Act (1998), the GDPR took the requirement of special protection for the personal data of children, including a requirement of parental

---

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

135 *Id.*

136 *See supra* note 34.

137 Mark Dawson, The Governance of EU Fundamental Rights 141 (2017).

138 *See supra* Part I.B.

139 GDPR, *supra* note 10, art. 47.

140 Daniel J. Solove and Paul M. Schwartz, Privacy Law Fundamentals 205 (4th ed. 2017).

consent.[141] 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.[142]

Finally, the CJEU functions as an important backstop to the dealmaking 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. Ireland has recently referred another important privacy case to this court; this matter, universally termed *Schrems II*, concerns the validity of both the standard contractual clauses and the Privacy Shield mechanism.[143]

B. Data Privacy Law in a Global Economy

Consider three incidents from the history of data privacy law. The first occurred at the international conference of data protection 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, one also held in October 2018. The contrast among these incidents serves to demonstrate not only a dramatic deepening of engagement between the U.S. and EU around data privacy, but a victory for the EU in the marketplace of ideas about data privacy. This section concludes by discussing a final overarching factor in the diffusion of EU privacy law, which is its creation of an easily transplantable regulatory model.

The Marketplace of Ideas. In October 1991 in Strasbourg, a law professor from the U.S. returned to the ongoing data protection commissioners' meeting, after taking a break, to be told that U.S. officials had just denounced him. 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.[144] 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.[145]

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."[146] The State Department representative told delegates and attendees that "the United

---

[141] *Id.* at 173–74.

[142] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (2009), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf; *see also* Ann Cavoukian, Privacy by Design in Law, Policy and Practice (2011), www.ontla.on.ca/library/repository/mon/25008/312239.pdf.

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

[144] For a discussion of this incident, see U.S. Official Blasts Law Professor's Description of Weak U.S. Privacy Law, 11 Privacy Times 1–3 (Number 18, Oct. 17, 1991).

[145] *Id.*

[146] *Id.*

States has considerable privacy protection, not omnibus, but nevertheless, considerable protection at both the federal and state level."[147] I was that professor, then teaching at the University of Arkansas (Fayetteville). The previous year I had become the first American to address the world's data protection commissioners at their twelfth annual meeting, held at the French Senate in Paris. In response to the criticism from the U.S. government in Strasbourg, I asked for an opportunity to respond and made two points: First, pursuant to the great American idea of the marketplace of ideas, the audience could decide whom to believe, and I certainly stood by my views on U.S. privacy law. Second, the criticism from the U.S. government represented "a very positive development."[148]

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, 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 come to 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 are moving in. If you 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 fifteen Americans here. And 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.[149]

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

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.[150] The delegation from the U.S. was not only numerous, but included such senior figures as the Secretary of Commerce;[151] the Ambassador to the EU; and the Chairperson of the FTC, along with three of his key staff members, including the head of the agency's privacy enforcement

---

147 *Id.*

148 *Id.*

149 *Id.*

150 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/.

151 *See* Wilbur Ross, Transatlantic Privacy Deal Is Vital to Trade, Financial Times (Oct. 17, 2018), https://www.ft.com/content/0f76f05e-d165-11e8-9a3c-5d5eac8f1ab4.

division.[152] The U.S. delegation also contained representatives from the Office of the Director of National Intelligence, the Department of Justice, and the State Department.[153] 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.[154] This Article has already discussed Cook's conviction that privacy is a human right. 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.[155] Stockpiles of personal data were serving "only to enrich the companies that collect them."[156] Cook spoke out against how a trade in personal information "has exploded into a data industrial complex" and praised the GDPR.[157] He flatly told the EU, "It is time for the rest of the world—including my home country—to follow your lead."[158] 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."[159]

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 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 Protection Act (CCPA) of 2018.[160]

The CCPA began as a ballot initiative slated for the November 2018 election. A series of high profile international, national, and state privacy

---

[152] *See* Fed. Trade Comm'n, Prepared Remarks of Chairman Joseph Simons, Second Privacy 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.

[153] Samuel Solton, US Taking Privacy Shield Deal Seriously, EU Officials Say, Euractiv (Oct. 18, 2018), https://www.euractiv.com/section/data-protection/news/us-taking-privacy-shield-deal-seriously-eu-officials-say/.

[154] Tim Cook, Remarks Before the International Conference of Data Protection & Privacy Commissioners (Oct. 24, 2018).

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] California Consumer Privacy Act, A.B. 375 (Cal. 2018) (amended by S.B. 1121 (Cal. 2018)).

scandals made the passage of this proposition likely. The initiative's sponsors also demonstrated their political savvy by including a super-majority requirement for amendment. 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. 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. 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.[161] The CCPA goes into effect on January 1, 2020.[162]

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 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.[163]

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 U.S. 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.

An Accessible Model. The GDPR and EU data protection principles have been applicable to legal systems and situations as diverse as Japan and the U.S. Yet, the EU did not set out to become the world's privacy cop. Its powerin 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.

---

161 *Id.*
162 *Id.*
163 *Id.*

As Weatherill notes, the EU's chief function is to manage the interdependence of its members.[164] 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. Abraham Newman summarized this initial process: "National legislation passed in the 1970s in several European countries was exported upward regionally . . ."[165] Bradford generally and correctly notes that the EU did not set out to engage in "regulatory imperialism," but merely to express domestic policy preferences.[166] The EU's influence has been greatly extended, however, by its fortuitous development of a regulatory model for privacy accessible for adoption outside the EU.

Omnibus privacy laws were the early choice for Member States pioneering in data protection. Such laws regulate both the private and public sectors and do so through general rules for data collection and use. These statutes can, in turn, be supplemented through sectoral laws where further regulations are needed. In contrast, the U.S. has favored information privacy statutes that regulate only individual sectors, such as credit reporting, video privacy, or financial institutions.[167] Unlike the EU, the U.S. lacks a general, safety-net omnibus regulation for personal information.

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. 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 of the price of joining the EU. 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."[168] 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.[169] In comparison to the sectoral-only U.S. approach, the simplified EU approach provides a highly attractive model for the rest of the

---

164 Weatherill, *supra* note 106, at 396.

165 Abraham Newman, Protectors of Privacy 3 (2008).

166 Bradford, supra note 25, at 6.

167 *See* Daniel Solove & Paul M. Schwartz, Information Privacy Law 786–88 (6th ed. 2017).

168 Joel R. Reidenberg, E-commerce and Transatlantic Privacy, 38 Houston L. Rev 717, 737 (2001).

169 *See generally* Alan Watson, Legal Transplants: An Approach to Comparative Law 94 (2d ed. 1974).

world. The most recent proof of its success as a transplant comes from Brazil, which in July 2018 enacted the first Brazilian data protection law. This statute is not only modeled on the GDPR, but shares the same name: *Lei Gerald de Proteção de Dados.*

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 U.S. In recent scholarship, Kristin Eichensehr envisions leading U.S. tech companies as large neutral entities, which she terms "Digital Switzerlands."[170] 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 U.S., Switzerland has enacted EU-style data protection laws and reached a coveted adequacy determination with the EU in 2000.[171] 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.[172]

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 U.S. 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 lesson, the EU's regulatory capacity reflects a complex interplay among its institutions, as well as adoption of outside influences. Bradford insightfully

---

[170] Kristen Eichensehr, Digital Switzerlands, 167 Penn. L. Rev. – (forthcoming 2019).

[171] 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518.

[172] As an example, the federal data protection law of Switzerland closely follows French and German models in this area of law. Eva Maria Belser et al, Datenschutzrecht 510–16 (2011).

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, 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. Second, 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. The global diffusion of EU data protection reflects a success in the marketplace of ideas.