NAVIGATING AN UNCERTAIN FUTURE: DATA TRANSFER AGREEMENTS IN THE AGE OF THE GDPR, PRIVACY SHIELD CHALLENGES, BREXIT & INTERNATIONAL TRADE TENSIONS

Taylor Treece*

Abstract

The ability to stay globally interconnected and to trade internationally is highly dependent upon data transfer agreements, which allow for the flow of data between different nations. However, the current U.S.-EU data transfer agreement is under mounting scrutiny and is at risk of invalidation, mere years after the last agreement succumbed to the same fate. This article seeks to explore why these agreements continue to struggle, what options are available for fixing these agreements (or going without), and how major world events could change the conversation about data transfer agreements moving forward. Providing a dynamic and comprehensive review of both the privacy principles and the greater political and economic motivators underlying the current challenges to these U.S. and European data transfer agreements, this article provides a practical guide for understanding and discussing where to next.

TABLE OF CONTENTS

* Buswell Fellow and Assistant Director of Research, Center for Legal & Court Technology, William & Mary Law School. Many thanks to my colleagues Iria Giuffrida and Fredric Lederer for their support, guidance, and helpful commentary on the drafts of this article. This work is supported by a grant from the Silicon Valley Community Foundation, funded by Cisco. Inc.

INTRODUCTION

The ability to create, store, and access data around the globe, at the touch of one's fingertips, is a main reason why the internet and data have become so important to modern society.[1] Data has facilitated the rise of globalism, enabling and easing channels of international communication and business.[2] At the same time, legal systems across the globe have struggled to keep pace with technological advances and sufficiently regulate the new world of interconnectedness. United States (U.S.) law has especially struggled to keep up with the expansive European Union (EU) data privacy rules and requirements, in part because of fundamental differences in international approaches that drive the creation of privacy law.[3] Beyond simply protecting privacy, the rules governing how data is shared are important because of their impact on, amongst other things, international trade. Since most, if not all, modern commercial transactions involve the transfer of data to some

[1] *See* Doron S. Goldstein, et al., *Understanding the EU-US "Privacy Shield" Data Transfer Framework*, 20 NO. 5 J. INTERNET L. 1, 1 (2016).
2. *Id.*
[3] Allison Callahan-Slaughter, *Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States*, 25 TUL. J. INT'L & COMP. L. 239, 240-46 (2016).

extent, international trade is dependent upon the ability to share and access data across borders. Currently, this is most often facilitated by data transfer agreements.[4] Several major events–including the finalization of "Brexit,"[5] the pending and anticipated challenges to the U.S.-EU Privacy Shield,[6] and the enforcement of the General Data Protection Regulation (GDPR)[7]–have upped the ante to find updated, effective multinational solutions to differing standards of data privacy protection, or to create contingency plans for a future without data transfer agreements.[8]

One of the major changes on the horizon is if and when the United Kingdom's (U.K.) exit from the EU is finalized.[9] While the details about leaving the EU are vague, it is at least known that, after invoking Article 50 of Treaty of Lisbon, there is a two year transition period before the U.K. will be officially "out" of the EU, unless the U.K. and EU come to a withdrawal agreement beforehand or the EU member states unanimously agree to an extension of time for exit negotiations.[10] Commentators on the process have remarked that sifting through which EU laws or rules the U.K. will keep and codify as U.K. law may take much longer than just the two year period.[11] In the interim, the U.K. remains a full member of the EU.[12] In any case, planning for a post-Brexit future of data management and

---

[4] Data transfer agreements, generally, set the conditions under which data may be legally transferred from one jurisdiction to another.

[5] *See generally* Linda G. Sharp, *Unshielded: The Effects of Brexit on Multinational Data Management*, 32 No. 17 WESTLAW J. CORP. OFFICERS & DIRS. LIAB. 1 (2017).

[6] *See* Paul Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, CQ ROLL CALL, Mar. 21, 2017; Paul Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, CQ ROLL CALL, Feb. 6, 2017.

[7] *See generally* Callahan-Slaughter, *supra* note 3, at 251-56.

[8] *See id.* at 256-58.

[9] *See* Sharp, *supra* note 5.

[10] The Lisbon Treaty art. 50(3).

[11] Jennifer Rankin, Julian Borger, & Mark Rice-Oxley, *What is Article 50 and Why is It So Central to the Brexit Debate?*, THE GUARDIAN (June 25, 2016), https://www.theguardian.com/politics/2016/jun/25/article-50-brexit-debate-britain-eu.

[12] Sharp, *supra* note 5, at 3.

transfers will be complex and time consuming because of the U.K.'s status as a core data management hub and its position as a bridge between the EU and other parts of the world.[13] As a result, it would be wise to start preparations earlier, rather than later, for data transactions with U.K., separate from the EU.[14]

As the U.S. has already seen, negotiating data transfer agreements with the EU is no easy task.[15] The current U.S.-EU data transfer agreement is the "Privacy Shield."[16] The Privacy Shield was formed in response to the 2015 invalidation of the prior agreement, known as the "Safe Harbor," by the Court of Justice of the European Union (CJEU).[17] The purpose of these data transfer agreements is to align the U.S. data privacy regime with the stronger protections for data privacy guaranteed by the EU.[18] The Privacy Shield attempts to strengthen the protections that existed under Safe Harbor, and bring the U.S. approach into closer conformity with EU requirements.[19] However, critics had already claimed that the Privacy Shield was insufficient to provide proper protections to EU citizens and EU citizen data prior to the enforcement of the GDPR.[20]As a policy matter, EU officials stated that they would not challenge the

---

[13] *See id.* at 1, 3-4.

[14] *See id.* at 5.

[15] *See, e.g.*, Will R. Mbioh, *Do the Umbrella Agreement and Privacy Shield Comply with the "Saugmansgaard Mandatory Requirements"?*, 20 N. 8 J. INTERNET L. 1 (2017).

[16] THOMAS F. VILLENEUVE, ET AL., *Chapter 2 Summary of Proprietary Rights*, CORPORATE PARTNERING: STRUCTURING AND NEGOTIATING DOMESTIC AND INTERNATIONAL STRATEGIC ALLIANCES loc. F.5.(a)-(c) (5th Ed. 2017 Supp.) (ebook).

[17] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r., 2015 E.C.R. I-1-35; *see also* Callahan-Slaughter, *supra* note 3, at 252-55.

[18] *Id.* ("Privacy Shield attempts to rectify Safe Harbors' shortcomings by placing safeguards on how U.S. authorities can access Europeans' data and creating a framework for resolving cases when Europeans challenge the use of their data as improper.").

[19] *Id*. at 253-54; Goldstein, *supra* note 1, at 18-20.

[20] Callahan-Slaughter, *supra* note 3, at 254-55; Goldstein, *supra* note 1, at 21; *see also* Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, *supra* note 6; Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, *supra* note 6.

adequacy of the Privacy Shield until summer 2017,[21] but this deadline has since passed and several challenges to the Privacy Shield have already been raised in European courts.[22] Even though the Privacy Shield managed to survive criticisms of and challenges to its compliance with the former EU Privacy Directive, it is unlikely that it will continue to be in compliance now that the GDPR came into full effect on May 25, 2018.[23] The GDPR includes updated privacy protections, in order to modernize the then current EU rules enacted in 1995, and accounts for advances in technology.[24] Importantly, the GDPR, which will be discussed in more detail in Part I, expands its definitions of personal data; carefully restricts who may control, process, and transfer data; gives EU residents the power to demand their data be deleted; sets narrow notification periods after data breaches; and establishes harsh penalties for violators of GDPR provisions.[25]

---

[21] Stephen Gardner, *EU Privacy Regulators Set Moratorium on Challenges to Data Transfer Pact*, BLOOMBERG BNA (July 26, 2016), https://bol.bna.com/eu-privacy-regulators-set-moratorium-onchallenges-to-data-transfer-pact/.

[22] One such challenge arose in Ireland. Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, *supra* note 6. However, this challenge was dismissed on November 22, 2017 for lack of standing under EU law at the time, which did not allow consumers to permit non-profits to sue and assert their privacy rights on their behalf. Daniel Felz, *Challenge to Privacy Shield Dismissed by EU General Court*, ALSTON & BIRD PRIVACY & DATA SEC. Blog (accessed Mar. 9, 2018). Notably, the GDPR expressly removes this standing issue and allows non-profit organizations to assert privacy rights on behalf of consumers. Since its passing, the Irish court has yet again referred the case to the CJEU, based upon an amended complaint focusing exclusively on Facebook's data transfers. Natasha Lomas, *Privacy Shield Now Facing Questions Via Legal Challenge to Facebook Data Flows*, TECH CRUNCH (Apr. 2018), https://techcrunch.com/2018/04/13/privacy-shield-now-facing-questions-via-legal-challenge-to-facebook-data-flows/.

[23] Goldstein, *supra* note 1, at 21 (citing Regulation 2016/679 of the European Parliament and of the Council of April 27, 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 Council Directive 95/46/EC, 2016 O.J. (L 119) 86, 87).

[24] *See* VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b).

[25] 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

Together, these three major events—Brexit, Privacy Shield Challenges, and the GDPR— offer a useful backdrop to examine the future of multinational data transfer agreements between three of the major players: the U.S., the U.K., and the EU. In reading the tea leaves to forecast what the resultant data transfer agreements may entail, it is therefore necessary to look at the relationships between the U.S. and the EU, the post-Brexit U.K. and the EU, and the possibility for a future U.S.-U.K. agreement.

I. THE GAP BETWEEN U.S. AND EU APPROACHES TO DATA PRIVACY

U.S. and EU data privacy approaches differ in the source, strength, and scope of data privacy protects. To better understand the challenges of striking data transfer deals between the U.S. and the EU, it is important to first examine the current state of the U.S. and EU data privacy regimes. This section first explores to the EU model, which contains clearer, more robust data privacy protections, before turning to the more complex web of the U.S. data privacy framework.

A. EU: From Directive to GDPR

Under EU law, privacy is considered a fundamental human right.[26] The resultant laws flowing from that right to privacy, including data privacy protections, are relatively firm and clear. To adequately protect data privacy in particular, the EU originally adopted a regulatory framework in the form of a directive, which member states were required to implement in their individual laws,

---

personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR") 2016 O.J. (L 119) 1 (copy available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN).

[26] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1, ch. I, Art. 8 (copy available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN). For a history of privacy, especially data privacy, as a human right as decreed by the European Convention on Human Rights, see Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Europe, and Canada*, 29 CONN. J. INT'L L. 257, 274-84 (2014).

to ensure compliance with the provisions of the EU law. The Data Protection Directive (hereinafter "the Directive") was the major source of EU law on data privacy since 1995.[27] Then, in 2016, the EU updated its data privacy rules by passing the GDPR, which went into effect in May 2018. Since the GDPR is a regulation, it became legally binding on all member states on the date it came into force.[28]

Both the Directive and the GDPR are primarily concerned with protecting "personal data." Personal data was defined under the Directive as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[29] Under the GDPR, the definition of "personal data" was adjusted to include

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[30]

Under either definition, the EU is concerned about "information that can be connected to an identifiable individual."[31] The definition of

---

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 13 (hereinafter "The Directive").
[28] GDPR, *supra* note 25.
[29] The Directive art. 2, *supra* note 27.
[30] GDPR, *supra* note 25 at § 4(1)).
[31] Raymond T. Nimmer, *§ 17:64.30.EU Data Protection Directive*, LAW OF COMPUTER TECHNOLOGY (May 2017 Update).

personal data is broad so as to include textual data, photographs, video and audio, and metadata (or, simply put, data about the data).[32] The EU seeks to protect personal data by regulating the quality of data collection, processing, and transfers.[33] In doing so, the EU strives to balance the simultaneous, and sometimes competing, goals of "protecting personal privacy and avoiding restrictions on the flow of personal data among member countries," while generally favoring limitations on the use of data to protect the interests of the individual to whom the data belongs.[34]

A core difference between the Directive and the GDPR is the nature of each piece of legislation and how it functions within the greater EU system. The general structure of the Directive set forth minimum requirements to safeguard data privacy, and then required the domestic laws of each member state comport with these EU standards.[35] If a member state could show that its existing framework and data privacy laws were sufficient to accomplish those goals, no further action was needed; if not, they would be required to pass additional laws to bring their domestic law into compliance with the Directive.[36] With this type of legislation, member states had more flexibility in determining how to accomplish the objectives contained in the Directive. However, the GDPR functions differently. As a regulation, rather than a directive, the GDPR is a binding legislative act in its own right, and applies as written to all member states.[37] To enforce the protections mandated by the GPDR, each member state must have a supervising authority to oversee the protection of citizen personal data.[38] These supervisory bodies[39] must be empowered to investigate data

---

[32] James, *supra* note 26, at 280.
[33] Nimmer, *supra* note 31.
[34] *Id.* For examples of the challenges posed by this policy to the private sector, see James, *supra* note 26, at 283-84.
[35] *See* REGULATIONS, DIRECTIVES AND OTHER ACTS, https://europa.eu/european-union/eu-law/legal-acts_en (last visited Sept. 26, 2018); James, *supra* note 26, at 280.
[36] *See* REGULATIONS, DIRECTIVES AND OTHER ACTS, *supra* note 35.
[37] *See id.*
[38] James, *supra* note 26, at 282.
[39] For a list, see DATA PROTECTION AUTHORITIES,

processing activities, to hear complaints from data subjects and issue public reports, and to intervene as necessary to block proposed data transfers or ensure data erasures.[40] The EU has its own, independent supervisory authority, the European Data-Protection Supervisor,[41] to oversee data protection throughout the EU, enforce privacy protections when international law or non-EU bodies are implicated, and monitor compliance with the EU data protection framework.[42]

The GDPR enhances the strength of EU privacy protections in several ways. First, it expands the territorial reach of EU data privacy law to encompass "those outside the EU who process data of EU residents in relation to the offering of goods and services to, or the monitoring of, EU residents."[43] This expands the regulation's reach beyond just EU citizens to include even non-EU citizens residing in the EU.[44] The GDPR imposes harsh punishments for mishandling data,[45] which could include sanctions "up to 4% of its worldwide revenue or 20 million euros (whichever is *higher*) for mishandling of personal and private data."[46] The GDPR requires specific data processing obligations, security, and notification measures for data breaches (including a notification period of 72 hours); written records of processing activities; cross border transfer provisions; increased accountability measures; deletion requirements; and, in some instances, appointed representatives from the certified organization to the EU.[47] In essence, the GDPR seeks to hold data controllers and processors accountable for the

---

http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm (last visited Sept. 24, 2018).

[40] *See* James, *supra* note 26, at 282.

[41] *See* EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/ (last visited Sept. 24, 2018).

[42] Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 469-70 (2016).

[43] VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b).

[44] *See id.*

[45] *Id*.

[46] Carole Basri & Mary Mack, *§ 24:8. Global data privacy and costs implications in eDiscovery in* EDISCOVERY FOR CORPORATE COUNSEL (Mar. 2017 update) (ebook).

[47] VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b).

data they possess, and it expects that they will be able to demonstrate their compliance for fear of harsh penalties.[48] Because the Privacy Shield was *already* coming under fire for failing to adequately protect data privacy rights as they existed under the Directive, it is unlikely that it would survive scrutiny now that these enhanced requirements are fully in force.[49]

B. Data Privacy in the U.S.

While a uniform federal government approach to data privacy would be constitutionally permissible,[50] the U.S. government has not enacted a comprehensive statutory scheme for asserting data privacy rights.[51] The U.S. has adopted a "sectorial" approach to data

[48] European Parliament: European Parliamentary Research Service, The Privacy Shield - Update on the State of Play of the EU-US Data Transfer Rules, PE 625.151 at 22 (July 26, 2018), available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2018)625151 (hereinafter, "Privacy Shield Update").

[49] Goldstein, *supra* note 1, at 21.

[50] *26.05. U.S. Data Privacy Law—In General*, 3 E-COMMERCE AND INTERNET LAW 26.05 (2016 update) ("Congress theoretically could yet adopt a general consumer privacy statute at some point in the future. In Reno v. Condon, the U.S. Supreme Court gave broad approval to the power of Congress to do so." (citing Reno v. Condon, 528 U.S. 141 (2000))).

[51] James, *supra* note 26, at 268-69. On September 25, 2018, however, the Trump administration announced a proposal to reform the U.S. data privacy model into a "risk-based," rather than rule-based, approach; the administration has opened up a request for comment period on the new proposal until Oct. 26, 2018. *See*, Alan Raul & Christopher Fonzone, *The Trump Admin. Approach to Data Privacy, and Next Steps*, LAW360 (Sept. 27, 2018, 1:53PM), https://www.law360.com/technology/articles/1086945/the-trump-admin-approach-to-data-privacy-and-next-steps?nl_pk=bf279ba6-78dd-4966-ab69-c44deef59ee6&utm_source=newsletter&utm_medium=email&utm_campaign=technology. This risk-based framework would be more comprehensive than U.S. data privacy laws currently, but seeks to create a more flexible, less prescriptive model for protecting data privacy (a clear, and seemingly intentional, departure from the comprehensive GDPR). *See id.* So far, these policy principles are in their infant stages, and lack key details (including, importantly, what privacy risks warrant protection). *See id.*

privacy.[52] The U.S. approach is, in this way, an outlier compared to the international trend towards comprehensive, top-down privacy legislation.[53] Instead, U.S. state and federal data privacy regulation has been slow to develop, has emerged largely in response to litigation or privacy breaches, and has been narrowly constructed, affecting only specific privacy issues.[54]

The generalized "right to privacy" in U.S. law is premised on a combination of Constitutional provisions, federal and state laws, and common law.[55] Though the U.S. right to privacy is often traced to the Bill of Rights in the Constitution, there is no constitutionally enumerated right to privacy.[56] The existence, breadth, and nature of U.S. data privacy protections are therefore more dependent on the type of information contained within the data and the jurisdiction with power over that data.[57]

Scholars have noted the trend in U.S. privacy law that the question of whether data privacy will be protected turns on whether the data involves "personally identified information" (PII).[58] While no uniform definition of PII exists in the U.S., it generally includes information like "social security number[s], residential address[es] and date[s] of birth."[59] Data that contains PII are typically protected in some way within the web of U.S. privacy law.[60] U.S. privacy rights generally can be further divided into categories based on "specific contexts (such as in connection with criminal investigations or in response to intrusive snooping by strangers)," "particular categories of information (such as tax returns, personal

[52] James, *supra* note 26, at 270 ("The usage of the term 'sectorial' with respect to privacy laws fundamentally refers to asymmetrical, industry-specific regulations, which are often very narrowly crafted and construed by the courts of law.").
[53] *Id.*
[54] *Id.* at 289.
[55] *26.05. U.S. Data Privacy Law—In General*, *supra* note 50.
[56] James, *supra* note 26, at 269.
[57] *26.05. U.S. Data Privacy Law—In General*, *supra* note 50.
[58] James, *supra* note 26, at 269.
[59] *26.05. U.S. Data Privacy Law—In General*, *supra* note 50.
[60] *James*, *supra* note 26, at 269.

financial data or medical records)," and "specific classes of people (such as children)."[61]

The protections originating in the U.S. Constitution are concerned with privacy rights against government intrusions, rather than violations of privacy committed by businesses or private individuals.[62] Federal laws have proceeded industry-by-industry, adopting narrow regulations.[63] The most notable federal laws and regulations that protect data privacy involve financial information, hacking and computer crimes, Federal Trade Commission (FTC) regulations, and consumer protections.[64] From there, specific U.S. laws that impact data privacy rights in various industries and contexts, including the Children's Online Privacy Protection Act of 1998 (restricting the collection and use of personal data from children), the Telecommunications Act of 1996 (regarding telemarking use of customer data), the Gramm-Leach-Bliley Act—also known as the Financial Services Modernization Act of 1999—(governing the use and distribution of private financial data), and the Fair and Accurate Credit Transactions Act of 2003 (enhancing protections in the Fair Credit Reporting Act of 1970 for personal data used in credit reporting).[65] Though federal breach notification laws have been proposed, none have been adopted yet.[66] Data processors can also come under FTC jurisdiction by posting privacy policies, and can then be found liable for deviating from their posted

---

[61] *26.05. U.S. Data Privacy Law—In General*, *supra* note 50.
[62] *Id*.
[63] James, *supra* note 26, at 290.
[64] *Id.* at 269-71.
[65] *Id.* at 271; *26.05. U.S. Data Privacy Law—In General*, *supra* note 50.
[66] Following the infamous Equifax data breach in early Fall 2017, it is conceivable that Congress will be motivated to enact a federal breach notification law; however, now months later, no such law has yet been adopted. *See, e.g.*, Selena Larson, *Senators Introduce Data Breach Disclosure Bill*, CNN TECH, Dec. 1, 2017, http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html; Joe Uchill, *Dem Reintroduces Breach Notification Law in Equifax Wake*, THE HILL (Nov. 18, 2017), http://thehill.com/policy/cybersecurity/351164-dem-reintroduces-national-breach-notification-law.

policy.[67] Recently, the federal government has also adopted the CLOUD Act, or the "Clarifying Lawful Overseas Use of Data Act," to amend the Stored Communications Act and specifically address the issue of data stored abroad by U.S. technology companies.[68] Rights advocates have criticized the law for its negative impact on privacy rights, arguing that it streamlines government access to private data stored abroad without sufficient protections to counterbalance its expansive reach.[69]

State laws and constitutions have included a variety of data privacy protections, using the same subject-matter-based framework as the federal laws. Some states have gone further than others in protecting privacy rights; for instance, California consistently maintains some of the strictest data privacy protections.[70] California is also one of only ten states to expressly add a privacy protection to its state constitution.[71] In California's example, this constitutional

---

[67] *26.05. U.S. Data Privacy Law—In General*, *supra* note 50. California has enacted laws requiring that companies post privacy policies, opening them up to FTC enforcement. *Id.*

[68] 18 U.S.C.A. § 2703, *amended by* PL 115-141 (2018) (hereinafter "CLOUD Act").

[69] Aaron Mak, *Congress Put the CLOUD Act in Its Spending Bill. What Does that Mean for Data Privacy?*, SLATE (Mar. 22, 2018), https://slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html.

[70] Divonne Smoyer, *The Growing Reach of State Attorneys General Over Data Privacy and Security Breach Incidents*, ASPATORE, March 2013. Additionally, California recently passed the California Consumer Privacy Act, expanding its data privacy protections in ways that mirror GDPR protections. *See* Cal. Civ. Code § 1798.160. However, the legislature can amend and edit provisions of this Act leading up to January 1, 2020, when the law is scheduled to come into effect; which protections will be included in the final version remains to be seen. *See, e.g.*, Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARVARD BUSINESS REVIEW (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

[71] *See* CAL. CONST. art. I, § 1. As of this article, the ten states include: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. Pam Greenberg, *Privacy Protections in State Constitutions*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-

provision protects against intrusions by both the government and private businesses, so long as the individual had a "reasonable expectation of privacy."[72] Though Missouri has not so broadly added a provision protecting privacy in its constitution, in 2014, it became the first state to explicitly protect against unreasonable searches and seizures of data or electronic communications in its state constitution.[73]

States, overall, have been most active in enacting laws regulating consumer protections and data privacy, including data breach notification laws.[74] All fifty states, and the District of Columbia, have now passed such laws.[75] The content of these laws vary, however, both in terms of how the statutes define the PII protected and the action required by entities that experience a data breach.[76] States have also passed data privacy protections in the form of unfair and deceptive trade practice acts.[77]

As seen above, neither the U.S. federal nor state laws directly or explicitly regulate "data privacy" or "personal data" in the comprehensive fashion characteristic of the EU approach; instead, both the state and federal laws regulate privacy through other subject matters that implicate data privacy. In tangentially regulating data privacy, or regulating only elements of data privacy, the state and

---

technology/privacy-protections-in-state-constitutions.aspx.

[72] Smoyer, *supra* note 70.

[73] Greenberg, *supra* note 71.

[74] For a list of each breach notification law, see *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[75] *See id*.

[76] Several charts and comparisons exist highlighting these difference. *See, e.g.*, Joseph J. Lazzorotti, et al., *State Data Breach Notification Laws: Overview of the Patchwork*, JACKSON LEWIS (Apr. 9, 2018), https://www.jacksonlewis.com/publication/state-data-breach-notification-laws-overview-patchwork; *State Data Security Breach Notification Laws*, MINTZ LEVIN (June 1, 2018), https://www.mintz.com/sites/default/files/media/documents/2018-09-18/UPDATED%20State%20Data%20Breach%20Matrix%20June%202018.pdf.

[77] *See, e.g.*, Smoyer, *supra* note 70.

federal governments have enacted laws regarding the same subject matter, but in different ways and with different requirements for how to manage that data depending on the circumstances. One of the challenges to the U.S. approach is that it "precipitates numerous, dissimilar terms and concepts," and, in some instances, contains multiple levels of overlapping, but not preempted, privacy laws.[78] So while the U.S. has recognizable trends in data privacy regulations, data privacy law in the U.S. is comprised of a complex, decentralized, overlapping web of protections.

II. FINDING AN AGREEMENT THAT STICKS FOR U.S.-EU DATA TRANSFERS

Because of the differences between the U.S. and EU approaches to data privacy, the U.S. and the EU have relied on a series of data transfer agreements to bridge the gap.[79] Data transfer agreements permit and govern the flow of information between nations by setting conditions for the transfer and processing of data by each nation's citizens.[80] However, these agreements have not always succeeding in providing adequate privacy protections.[81] Understanding why past agreements have failed can help predict whether the Privacy Shield will be found similarly inadequate[82] and how the GDPR will change the discussion about future data transfer agreements.[83]

A. History of Data Transfer Agreements: From the Not-So-Safe Harbor to the Privacy Shield

Beginning in 1995 with the enactment of the European Union's Data Protection Directive,[84] the divergence between the comprehensive EU data privacy protections and the looser, decentralized, *ad hoc* U.S. approach to data privacy law has steadily

[78] James, *supra* note 26, at 270-71.
[79] *See infra* Part II.A.
[80] *See* Goldstein, *supra* note 1, at 18.
[81] *See infra* Part II.A.
[82] *See infra* Part II.B.
[83] *See infra* Part II.C.-E.
[84] The Directive, *supra* note 27.

widened.[85] In response, the U.S. and EU have struck agreements, such as the Safe Harbor Agreement[86] or the Umbrella Agreement,[87] to facilitate data transfers between EU member states and the U.S., while preserving the heightened standards of data privacy present in EU law. Ultimately, the regulation gap between the EU and the U.S. culminated in the 2015 *Schrems* decision by the CJEU, invalidating the Safe Harbor Agreement and espousing principles of data privacy law that must be present for non-EU nations to meet EU data privacy standards.[88]

In response to *Schrems*, the Obama administration scrambled to renegotiate a data transfer agreement with the EU.[89] The solution was the "Privacy Shield" framework, formally adopted in July of 2016, which governs data transfers and processing by companies and organizations.[90] The Privacy Shield allows U.S. companies to self-certify to the U.S. Department of Commerce that the company commits to abide by core EU data privacy principles;[91] the Privacy Shield, as well as subsequent legislation, provides for federal oversight, enforcement mechanisms, and legal recourse for mishandling EU citizen data and other violations of EU privacy principles.[92]

---

[85] Callahan-Slaughter, *supra* note 3, at 240-46.

[86] *See* Commission Implementing Decision of July 12, 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, 2016 O.J. (L 207) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN; Privacy Shield Framework, 81 Fed. Reg. 51041 (Aug. 2, 2016) (hereinafter "Privacy Shield").

[87] Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, 2016 O.J. (L 336) 3, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.336.01.0003.01.ENG (hereinafter "Umbrella Agreement").

[88] *See* Case C-362/14, Maximillian Schrems v. Data Protection Comm'r., 2015 E.C.R. I-1-35.

[89] Callahan-Slaughter, *supra* note 3, at 552-55.

[90] *Id.* at 554-55.

[91] Goldstein, *supra* note 1, at 19-20.

[92] *Id.* at 1, 18-21.

While the Privacy Shield resembles the Safe Harbor agreement in many ways, several provisions were added to it in an attempt to resolve the previous insufficiencies of Safe Harbor.[93] First, the Privacy Shield tightens restrictions on "onward transfers," or transfers of personal data to third parties, requiring that onward transfers only occur for "limited purposes" and only under contracts that provide the "same level of protection" as the Privacy Shield.[94] Second, the Privacy Shield requires that organizations update their privacy policies to notify users of "contact information for an independent dispute resolution provider; notice of a new arbitration right; a disclaimer that disclosures may be made to public authorities for law enforcement purposes; and that the organization remains liable for onward transfers."[95] Once the purpose for which data was collected has been served, organizations are now required to delete the data.[96] Under the Privacy Shield Framework, the U.S. Department of Commerce will exercise heightened regulatory oversight, which includes "verifying organizational compliance with the Privacy Shield and conducting periodic ex officio reviews of certifying organizations."[97] In part to facilitate oversight and review, organizations certified under the Privacy Shield must maintain records about their Privacy Shield-related practices.[98] Though not an express provision of the Privacy Shield, approval of the Privacy Shield was conditioned on the extension of judicial redressability to European citizens.[99] In response, the U.S. enacted the Judicial Redress Act, which extends the U.S. Privacy Act of 1974 to European citizens.[100]

---

[93] *See id.*

[94] Privacy Shield, *supra* note 86.

[95] Goldstein, *supra* note 1, at 19; *see also id.*

[96] Privacy Shield, *supra* note 86.

[97] Goldstein, *supra* note 1, at 19; *see also id.*

[98] Privacy Shield, *supra* note 86.

[99] Callahan-Slaughter, *supra* note 3, at 255-56.

[100] Judicial Redress Act of 2015, 5 U.S.C. § 552a. This act expanded the privacy protections to "covered person(s)" who are citizens of a "covered country," as designed by the Attorney General (with approvals by the Secretary of State, Secretary of the Treasury, and Secretary of Homeland Security). *Id.* The Attorney General subsequently designated the EU among the "covered countries." Attorney

B. Cracks in the Shield

Even with these added protections, critics have doubted the efficacy of the Privacy Shield, claiming that the safeguards for data privacy are still inadequate compared to EU requirements, even under the previous, lower standards of the Directive.[101] While the Privacy Shield introduced new requirements on U.S. organizations and authorized enhanced regulatory oversight, the chief concerns are that organizations will continue their current practices and that regulatory agencies will not, in practice, enhance their enforcement of Privacy Shield requirements.[102] This fear is in part due to U.S.'s failure to adequately enforce even the lesser protections afforded by the Safe Harbor.[103]

The Privacy Shield is subject to annual review by EU authorities, beginning September 2017.[104] The CJEU has refrained from hearing challenges to the Privacy Shield at least until Summer 2017, presumably to observe the Privacy Shield in action before rending a decision on the sufficiency of its protections.[105] But now that 2017 has come and gone, the Privacy Shield is increasingly vulnerable to critics who would attack its adequacy, whether by annual EU review or by judicial processes. Already, a case in the Irish courts challenged the Privacy Shield, claiming that it is invalid and insufficient to assure compliance with EU law under the

---

General Order No. 3824-2017, "Judicial Redress Act of 2015; Attorney General Designations," 82 Fed. Reg. 7860 (Jan. 23, 2017).

[101] *See, e.g.*, Mbioh, *supra* note 15; Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, *supra* note 6; Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, *supra* note 6.

[102] *See, e.g.*, Mbioh, *supra* note 15; Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, *supra* note 6; Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, *supra* note 6.

[103] *Cf.* Case C-362/14, Maximillian Schrems v. Data Protection Comm'r., 2015 E.C.R. I-1-35.

[104] Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, *supra* note 6.

[105] Goldstein, *supra* note 1, at 21 (citing Stephen Gardner, *EU Privacy Regulators Set Moratorium on Challenges to Data Transfer Pact*, BLOOMBERG BNA (July 26, 2016), https://bol.bna.com/eu-privacy-regulators-set-moratorium-onchallenges-to-data-transfer-pact/).

Directive.[106] Though this case was ultimately dismissed for lack of standing, the Privacy Shield is far from out of the woods. The Irish case was dismissed because the Directive did not grant standing to third parties, such as privacy rights advocates, asserting claims on behalf of consumers.[107] However, one new provision of the GDPR expressly grants standing to non-profit organizations to bring suits on behalf of consumers regarding privacy breaches—which resolves the standing deficiency that defeated the Irish challenge.[108] So with the standing question seemingly out of the way, the current challenge in the Irish courts, also brought by Maximilian Schrems (hereinafter "*Schrems II*"), to the Privacy Shield has been renewed and will test whether the Privacy Shield lives up the heightened data privacy requirements under the GDPR.[109]

Recent resolutions and reports by the European Parliament suggest that the Privacy Shield may not last much longer. The European Union has been vocal, such as during the first annual review of the Privacy Shield in September 2017, that it had reservations about the Privacy Shield and made recommendations for improvements.[110] Though the Privacy Shield was deemed "adequate" in this first review, the review stressed the need for "tougher monitoring of companies' compliance by the US Department of Commerce; appointment of a [Privacy Shield] Ombudsperson to deal with Europeans' complaints concerning access to personal data by US authorities as well as appointment of the missing members of the Civil Liberty Oversight Board" to continue to adequately comply with the privacy standards under the

---

[106] C-311/18, Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, 2018/C 249/21 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CN0311&from=EN); *see* Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, *supra* note 6.

[107] *See Felz*, *supra* note 22.

[108] *See* GDPR, *supra* note 25, at art. 80; *see also* Lomas, *supra* note 22.

[109] Goldstein, *supra* note 1, at 21; Lomas, *supra* note 22.

[110] Privacy Shield Update, *supra* note 48.

Directive.[111] In July 2018 (now with the GDPR in effect), the European Parliament adopted a resolution citing persistent concerns with the Privacy Shield, calling on the Commission to investigate the status of the Privacy Shield, and ultimately requesting it suspend the Privacy Shield.[112] The European Parliament Resolution concluding that the Privacy Shield was not adequate to protect rights guaranteed by the GDPR is non-binding, but may be a sign of what is to come.

In addition to the overarching and continuing concerns from the first annual review, other events, like the Facebook/Cambridge Analytica scandal[113] or the passage of the CLOUD Act—both of which have aroused skepticism in the European community about the U.S. government and private sector commitments to meaningful data privacy protections—, have raised ever more red flags about continuing the Privacy Shield.[114] Further complicating the matter, recent U.S. trade policies, especially tariffs on foreign goods, from the Trump administration have caused mounting tensions internationally, including with the EU.[115] While a trade deal

---

[111] European Commission Press Release, *EU-US Privacy Shield: First review shows it works but implementation can be improved*, 25 (Oct. 18, 2017, IP/17/3966).

[112] *Id.* at 23. For the full text of the resolution, see European Parliament Resolution of 5 July 2018 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield (2018/2645(RSP)), EUR. PARL. DOC. P8_TA-PROV(2018)0315 (available at www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN).

[113] *See, e.g.*, Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, NY TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[114] Privacy Shield Update, *supra* note 48.

[115] *See, e.g.*, Jack Ewing, *Europe Feels the Squeeze of the Trump Trade Tariffs*, NY TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/business/economy/europe-trade-trump-tariffs.html; *Weekend: EU-US Trade War?*, BBC WORLD SERVICE (June 23, 2018), https://www.bbc.co.uk/programmes/w172w71spy7db3y; Ben Sills & Richard Bravo, *Europe's Retaliation Takes U.S. Trade Tensions to the Next Level*, BLOOMBERG NEWS (June 22, 2018), https://www.bloomberg.com/news/articles/2018-06-22/europe-s-retaliation-takes-u-s-trade-tensions-to-the-next-level; '*US Playing a Dangerous Game'*,

brokered near the end of summer 2018 has, for the time being, avoided an "all-out trade war" between the U.S. and EU,[116] the situation is far from completely resolved.[117] Even as the deal was announced, commentators expressed concern that the Trump administration will not follow through with the deal as time goes on, citing to examples set by the Trump administration in similar situations with Chinese tariff tensions.[118] Should trade tensions escalate again, the GDPR might prove a useful tool against the U.S. If the Privacy Shield were invalidated, U.S. businesses would struggle to continue trading, in any industry, with EU countries, as almost every business transaction would necessitate the transfer of data with the EU.[119] Any U.S. company that decided to trade anyway

---

BBC NEWS (June 1, 2018), https://www.bbc.com/news/av/business-44336449/us-playing-a-dangerous-game-eu-trade-chief-says.

[116] *See, e.g.*, *All Things Considered: Trump Announces Trade Deal With European Commission That Will Lower U.S.-Europe Tension*, NPR RADIO (July 25, 2018), https://www.npr.org/2018/07/25/632436795/trump-announces-trade-deal-with-european-commission-that-will-lower-u-s-europe-t; Mark Landler and Ana Swanson, *U.S. and Europe Outline Deal to Ease Trade Feud*, NY TIMES (July 25, 2018), https://www.nytimes.com/2018/07/25/us/politics/trump-europe-trade.html; *The World Tonight: US EU Deal to Avoid Trade War*, BBC RADIO 4 (July 25, 2018), https://www.bbc.co.uk/programmes/b0bbn6z2.

[117] *See, e.g.*, Damian Paletta & Jeanne Whalen, *Trump, E.U. Announce Deal to Avert Escalation of Trade Tension*, WASH. POST (July 25, 2018), https://www.washingtonpost.com/business/economy/trump-pushes-25-percent-auto-tariff-as-top-advisers-scramble-to-stop-him/2018/07/25/f7b9af04-8f8a-11e8-8322-b5482bf5e0f5_story.html?noredirect=on&utm_term=.c9d910b891a4 (acknowledging that "questions remain" as "Trump did not definitively agree to suspend steel and aluminum tariffs," "Juncker did not agree to reduce tariffs on U.S. car imports," and no "specific agreement on existing tariffs" was brokered).

[118] *See, e.g.*, Landler & Swanson, *supra* note 116 ("It was hard to say, given Mr. Trump's bluster and unpredictable negotiating style, if the agreement was a genuine truce or merely a lull in a conflict that could flare up again. Twice, Mr. Trump's aides have negotiated potential deals with China, only to have him reject them and impose further tariffs."); Paletta & Whalen, *supra* note 117 (quoting former White House economist Chad Bown that "[w]ords only mean so much" and "[w]e could see a tweet in 20 minutes to completely reverse all of this" while acknowledging that the agreement was itself a "positive sign").

[119] *Cf.* AJ Agrawal, *Why Data is Important for Companies and Why Innovation is On the Way*, INC. (Mar. 24, 2016), https://www.inc.com/aj-agrawal/why-data-is-important-for-companies-and-why-innovation-is-on-the-way.html (discussing

in violation of GDPR provisions could then be hit with huge penalties in retaliation.[120] The tensions surrounding the Privacy Shield, then, are mounting not simply because of data protection concerns, but because of the overarching state of U.S. and EU relations. Therefore, it is important not to consider data regulation in a vacuum, but also in the greater, dynamic context of both international politics and economics.

C. *Forging an Agreement in a Post-Shield Future*

In looking towards the future of U.S.-EU data relations, the first question to be addressed is what standards, requirements, and regulations the agreements must include. One of the greatest difficulties in predicting, and thereby planning for, the future of data transfer relations between the U.S. and EU is deciphering what exactly the agreement must safeguard, and how, to satisfy EU privacy standards and withstand potential future legal challenges.[121]

One place to start is by looking at where the Safe Harbor went wrong. Because a core tenant of EU data privacy agreement is the "adequacy principle," which requires non-EU countries receiving EU data transfers to provide an "adequate level of protection," seeing what made the Safe Harbor inadequate informs whether the changes between the Safe Harbor and Privacy Shield brought the Privacy Shield within the realm of "adequacy" under the Directive standards.[122] Starting with the question of whether the Privacy Shield fixed the defects present in the Safe Harbor determines whether alterations to the Privacy Shield need only consider the new requirements under the GDPR, or whether it must make more fundamental changes.

The *Schrems* case, in invalidating the Safe Harbor, laid out several principles of data privacy under EU law to provide further

---

the extent to which consumers are generating data and ways that businesses are relying on data in their daily operations).

[120] *See* GDPR, *supra* note 25.

[121] *See* Mbioh, *supra* note 15, at 24.

[122] Callahan-Slaughter, *supra* note 3, at 246.

guidance on the adequacy requirement.[123] This decision recognized that the adequacy principle does not require other countries to maintain *identical* levels of protection as in the EU, but that adequacy "must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union."[124] In doing so, *Schrems* noted that the other country, seeking to access and control EU citizen data, must demonstrate its adequacy, must enact "applicable rules" that are "designed to ensure compliance" with the EU regulations, and must have mechanisms for the EU to periodically check in on the ongoing adequacy of these rules.[125]

Turning to contemporary Privacy Shield challenges, these principles shed light on what questions European courts will ask when evaluating adequacy. They demonstrate that the CJEU is concerned not only with what data transfer agreements contain in their provisions, but also how they are enforced in practice.[126] But looking at the *Schrems* principles alone is not likely to reveal what new agreements will need to contain to remain adequate under the new European standards. To begin with, *Schrems* was articulating principles based on the Directive, which allows greater flexibility in how countries, even EU countries, comply with privacy standards compared to EU regulations, like the GDPR.[127] When it comes to the specifics of how to adequately protect data, the GDPR provides more concrete guidelines for compliance moving forward than the *Schrems* principles alone.[128]

---

[123] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r., 2015 E.C.R. I-1-35.
[124] *Id.*
[125] *Id.*
[126] *See id.*
[127] *See supra* notes 35-42 and accompanying text.
[128] *Compare* VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b) (describing the specific provisions enacted by the GDPR, which will go into full effect in May 2018) *with* Mbioh, *supra* note 15 (deciphering the standards proclaimed in the *Schrems* case and in the article by Advocate General Saugmandsgaard).

Looking at what has changed between the Directive and the GDPR provides a roadmap for ways the Privacy Shield framework could be adjusted and amended.[129] Specifically, a potential future agreement must require U.S. organizations and companies to increase recording and reporting of data privacy processing activities, increase cybersecurity protections, update notification measures following data breaches, strengthen cross border transfer provisions (including liability imposed for breaches by third party transferees), delete data after the purpose for which data was collected is complete, and, in some cases, provide appointed representatives to the EU in the event of a breach.[130] Equally important, the U.S. must address the major concern of actually enforcing these promises by U.S. organizations and promises, which may necessitate the creation of supervising agencies or other forms of federal legislation that provide for enforcement mechanisms.[131] An agreement that contains all of the previsions listed in writing, but which in reality is never enforced, is just as likely to be declared inadequate, just as the Safe Harbor.

An even more difficult question than *what* to require in a future U.S.-EU agreement, however, is *how* to go about legislating and regulating these increased GDPR requirements. A recurring problem in developing data transfer agreements has been the fundamentally different approaches that the EU and the U.S. have taken in forming their laws and policies.[132] This is largely what leads to the distrust in the EU that the U.S. will follow through on promises made in a data transfer agreement to protect EU citizen data. The EU views data privacy rights as part of the fundamental human right to individual privacy.[133] As such, the EU affords data

---

[129] *Cf.* VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b).
[130] *See id.*
[131] *See, e.g.*, Mbioh, *supra* note 15; Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, *supra* note 6; Merrion, *Irish High Court Hears Pivotal U.S.-EU Data Privacy Case Starting Tuesday*, *supra* note 6.
[132] *See* Callahan-Slaughter, *supra* note 3, at 240-46.
[133] *See id.* at 240 (citing THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA: RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY 250 (2014)).

privacy rights the most stringent protections, and uses centralized, top-down regulations to safeguard user privacy.[134] The EU regulations assume, in evaluating the adequacy of non-EU data protections, that these foreign nations have also adopted a regulatory approach, rather than a litigation approach, that has created supervisory bodies to monitor data privacy protections.[135]

Meanwhile, U.S. values of federalism, limited government, and narrowly constructed legislation have led U.S. lawmakers to take a decidedly different approach—that is, not a strictly regulatory approach—to data privacy legislation.[136] The U.S. has favored market constraints over government intervention,[137] and U.S. laws on data privacy have most often come as a reaction to high profile data privacy breaches.[138] The right to privacy in the U.S., generally, is "limited" to "specific areas where protection is deemed necessary," as recognized in a patchwork of legal sources including the First, Fourth, Fifth, and Fourteenth Amendments of the Constitution, federal and state legislation, and market self-regulations.[139]

As a result of the differing values surrounding privacy law, and the sources through which those rights are derived, it may be difficult for the U.S. to continue to accept a further expansion of data privacy rights as a matter of public policy.[140] Were the right to privacy an enumerated right protected in the Constitution, it may be easier to develop U.S. law that parallels the EU treatment of privacy as a fundamental right.[141] As an unenumerated right, the U.S. is

---

[134] *Id.* at 240-42.
[135] *See* Nimmer, *supra* note 31.
[136] *Id.* at 243-44.
[137] *Id.* at 243.
[138] *Id.*
[139] *Id.* at 243-44 (citing THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA: RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY 248-49 (2014)).
[140] *See id*. That said, the U.S. is currently pursuing a Swiss-U.S. "Privacy Shield" containing even stricter restrictions that the U.S.-EU Privacy Shield. *See* Paul Merrion, *Swiss-U.S. Privacy Shield Applications Now Underway*, CQ ROLL CALL, Apr. 12, 2017.
[141] *Cf.* Callahan-Slaughter, *supra* note 3, at 240-46.

likely to view even expansions of the right to individual privacy as government overreach.[142] One reason for this is that the U.S., generally and historically, values capitalism and limited regulation of markets, which is at odds with the comparatively stringent restrictions on businesses required by the EU through the GDPR.[143] Already, Congress has expressed discomfort at expanding U.S. law in this top-down fashion to fully encompass the EU privacy requirements.[144] Ultimately, these diametrically opposed positions on how to regulate data privacy may foreshadow that data transfer agreements between the U.S. and EU will continue to face challenges, regardless of their substantive content, until the parties can appreciate and negotiate within the realities and priorities of different legal systems.

D. Alternatives to Meeting EU Requirements: Possible, But Not Too *Promising*

While data transfer agreements significantly ease channels between nations, it is still entirely possible to maintain trade and to share data across boarders in the absence of data transfer agreements. Some alternatives to the Privacy Shield, and transnational data privacy agreements overall, already exist. The GDPR continues to recognize two existing, alternative solutions for data privacy compliance: (1) Binding Corporate Rules, and (2) Standard Contractual Clauses. These alternatives provide an important safeguard in case data transfer agreements become increasingly difficult to negotiate, but each alternative has its own set of drawbacks.

Binding Corporate Rules (BCRs) are "binding 'gold standard' rules for an organization's data privacy procedures and compliance."[145] BCRs are well suited for organizations with

---

[142] Ironic as it might be for government overreach to come in the form of giving people too many rights, in a sense. However, under the U.S. approach, firm data privacy restrictions are more likely to be seen as encroaching on free markets and burdening business transactions. *Cf. id.*

[143] *See id.*

[144] *See id.* at 255-56.

[145] VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b).

"complex international data flows,"[146] as BCRs typically require "some level of EU operations."[147] In fact, BCRs require a lengthy approval process by EU data protection authorities.[148] When weighing the value of BCRs from the U.S. perspective, BCRs allow for more market self-regulation, because they are voluntarily undertaken by businesses and organizations, and minimize U.S. government supervision.[149] BCRs have been unpopular relative to other data transfer frameworks, however, in part because the "practical application [of BRCs] proved costly and burdensome."[150] So while BCRs provide an alternative to transnational agreements that may be consistent with U.S. regulatory and privacy values in principle, BCRs are not suitable for all organizations and may not be preferred even by eligible organizations because of the cost and administrative difficulty.

The other alternative framework is often called the "Standard Contractual Clauses" (SCCs). SCCs can occur in one of two ways: either the organization can use one of the prescribed forms created and disseminated by the EU Commission;[151] or it can enter into individually negotiated contracts (so long as the contract is consistent with EU legal data protection principles), and then file the contract with and seek the approval of the competent EU data protection authorities.[152] Especially following the invalidation of Safe Harbor, many U.S. businesses and organizations switched to

---

[146] *Id.*

[147] Goldstein, *supra* note 1, at 20.

[148] *See id.* at 20 n.20.

[149] Joanna Kulesza, *Walled Gardens of Privacy or "Binding Corporate Rules?": A Critical Look at International Protection of Online Privacy*, 34 U. ARK. LITTLE ROCK L. REV. 747, 759 (2012).

[150] *Id.* The GDPR also took steps to simplify the process of seeking and using BCRs. *See* Privacy Shield Update, *supra* note 48. However, it is too soon to tell whether this updated process will impact the popularity of BCRs as an alternative going forward.

[151] For examples of SCC forms approved by the EU, see MODEL CONTRACTS FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (last visited Oct. 1, 2018).

[152] VILLENEUVE, ET AL., *supra* note 15 loc. F.5.(b).

SCCs to ensure legal compliance with EU restrictions.[153] SCCs are, nevertheless, cumbersome for organizations, and do not necessarily guarantee compliance.[154] The Irish challenge discussed earlier in this article sought to invalidate not only the Privacy Shield but also SCCs as inconsistent with EU data privacy protection standards.[155] Now that the standing issue that prevented the CJEU from rendering a decision about SCCs has been resolved by the GDPR, the Irish high court is continuing with the *Schrems II* challenge and has referred a list of eleven questions to the CJEU for a preliminary ruling.[156] Until such a decision, the fate of SCCs as a long term solution still hangs in the balance.

E. Last Resort: Data Isolationism as a Bargaining Tool, or a Reality

In the absence of a workable EU-U.S. privacy agreement or viable alternatives (either the BCRs or SCCs), the remaining option would be a trend towards increased data isolationism. On its face, the idea of retreating back into closed borders in the age of free-flowing data, technological, and information transfers seems nigh inconceivable.[157] However, as previously mentioned, trade tensions have been rising between the U.S. and EU, which makes the

---

[153] *See* Merrion, *After Lengthy Trial, Decision Awaited in Case Testing U.S.-EU Data Pacts*, *supra* note 6.
[154] *See id.*
[155] *See id.*
[156] C-311/18, Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, 2018/C 249/21 (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CN0311&from=EN). The CJEU has jurisdiction over matters pertaining to EU law. *See* COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU), https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en (last visited Sept. 27, 2018). Generally, within the structure of the EU, cases can either be brought directly to the CJEU when dealing with complaints about EU institutions, or indirectly through member state courts, who then refer the case to the CJEU either as a whole or through questions about the case requesting guidance on how to interpret EU law. *See id.*
[157] *See* Goldstein, *supra* note 1, at 1.

possibility of ceasing data transfers as a retaliatory trade tactic more likely.[158] This threat then begs the questions of what a world without data transfer agreements would look like.

One answer to that question can be found in recent experiments with isolationist tactics, like blocking statutes and data retention laws. Leading up to January 2017, several countries, including EU nations like Germany and France—who are known as progressives in the field of data privacy[159]—had enacted statutes requiring that all data created or accessed within the country to be stored locally, within the country's territorial boundaries.[160] The purpose of these statutes was to ease access, especially government access, to user data, as the statutes avoided the need for multinational agreements or Mutual Legal Assistance Treaties.[161] Similarly, EU countries, like Germany and France, have recently called for relaxing EU data privacy regulations in response to the acts of international terrorism throughout Europe and the world.[162]

In January, the CJEU opinion in *Tele2 Sverige AB v. The Swedish Post and Telecom Authority* invalidated laws that required companies to retain personal data to enable ease of government access as "in breach of EU-wide law."[163] This strongly suggests that the CJEU will look upon efforts to stockpile user data within a country's territorial boundaries unfavorably, and that the court will regard this type of data isolationism as inherently at odds with EU data privacy principles for the purposes of determining privacy framework "adequacy."[164] But as a last resort in the event that all attempts to reconcile U.S. and EU data privacy law fail, data

---

[158] *See supra* notes 115-120 and accompanying text.
[159] *See* Callahan-Slaughter, *supra* note 3, at 258.
[160] *See* Stephen Gardner, *EU Top Court Rules Companies Can't Be Forced to Retain Data*, BNA, Jan. 5, 2017.
[161] *See id*.
[162] Callahan-Slaughter, *supra* note 3, at 257-58.
[163] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v. The Swedish Post and Telecom Authority*, CJEU, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537578084665&uri=CELEX:62015CJ0203.
[164] *See id.*

localization statutes would at least allow the U.S. to function by preserving its own access to necessary data.[165]

However, this is an imperfect approach, even for a fail-safe, because of the EU restrictions on "onward transfers" to third parties.[166] Ultimately, this gives the EU great coercive power to control the trade deals between the U.S. and other countries, even those not directly under EU control. If the U.S. were to break completely with the EU data privacy regulations, then the EU restrictions would likely impose an ultimatum on middlemen countries: either cease data transfers to the U.S., or risk the consequences of violating EU privacy law.[167]

In the alternative, because modern society often presupposes the easy, free flow of data and information, perhaps merely the threat of invoking this doomsday isolationism would be enough to force the EU back to the bargaining table, should negotiations for a future data transfer agreement break down to this extent.[168] However, as discussed in the context of trade tensions between the U.S. and EU, this tool can just as easily be wielded against either party.[169] But, as will be discussing in Part IV, the isolationist bargaining tool may gain even more power in the U.S.'s favor should the U.S. and the post-Brexit U.K. align to drive down EU mandated regulations on business.[170] Perhaps the combined effect of the U.S.-U.K. market power would be sufficiently threatening to the EU economy that it might garner a more favorable agreement, or, at the very least, slow down the string of invalidation challenges before the EU courts.[171]

---

[165] *Cf. id.*
[166] *See* Goldstein, *supra* note 1, at 18.
[167] *See id.*
[168] *Cf.* Callahan-Slaughter, *supra* note 3, at 239-40.
[169] *See supra* notes 115-120 and accompanying text.
[170] *See infra* Part IV.
[171] *See* Belton Zeigler, Andrew Kimble & Malcolm Dowden, *Data Protection Law — A Broken Shield*, 34 No. 20 WESTLAW J. COMPUT. & INTERNET 2, 3-4 (2017). Note, however, that the U.K. referendum is non-binding, though the U.K. government decided, in the wake of the referendum, to start the process of exiting the EU. During the summer 2018, the possibility of a second "Brexit" referendum was proposed, which could reverse the U.K.'s stance on exiting the EU. *See, e.g.*,

III. NEGOTIATING A "BREXIT" STRATEGY: U.K. & EU AGREEMENTS

The referendum vote through which 51.9% of U.K. citizens elected to leave the EU sent shock waves through both the U.K. and the international community.[172] Commonly called "Brexit,"[173] the process of the U.K. exit from the EU promises to be a complex, arduous undertaking. Article 50 of the Treaty of Lisbon, which governs withdrawals from the EU, is so short and lacking in detail that some say it is apparent that the drafters did not anticipate that any country would invoke the provision.[174] The U.K. has been pressing forward on the resolution to leave the EU;[175] once the U.K. invoked Article 50—which it did on March 29, 2017—there is a two-year process of negotiations with EU delegates.[176] After those two years, the U.K. will exit the EU (deal or no deal), unless the remaining EU states unanimously approve an extension to allow negotiations to continue.[177] At least one U.K. government official

---

A Second Brexit Referendum is Back in Play, THE ECONOMIST (July 19, 2018), https://www.economist.com/britain/2018/07/19/a-second-brexit-referendum-is-back-in-play; Tom Edgington, *Brexit: How Would a Second EU Referendum Be Held?*, BBC NEWS (July 16, 2018), https://www.bbc.com/news/uk-44847404. As discussed below in Part III, the process of exiting the EU is ill-defined and the question of whether the U.K. could cease exiting procedures is currently unsettled. *See infra* Part III. Likewise, the question of whether the U.K. could even stop the Article 50 process of exiting the U.K. once it has been triggered is also unsettled, and would likely become a question for the CJEU. *Cf. infra* Part III.

[172] *See* Alex Hunt & Brian Wheeler, *Brexit: All You Need to Know About the UK Leaving the EU*, BBC NEWS (Mar. 30, 2017), https://www.bbc.com/news/uk-politics-32810887.

[173] "[Brexit] is a word that has become used as a shorthand way of saying the UK leaving the EU - merging the words Britain and exit to get Brexit." *Id.*

[174] *See* Sharp, *supra* note 5, at 2; *see also* The Lisbon Treaty art. 50 (consisting of only 5 short provisions and 261 words).

[175] On March 29, 2017, U.K. Prime Minister Theresa May triggered Article 50, which means that the U.K. is currently scheduled to leave the EU on March 29, 2019. Hunt & Wheeler, *supra* note 172.

[176] *Id.*

[177] The Lisbon Treaty art. 50(4).

has predicted that, to fully complete exit negotiations, the process could take up to six years.[178]

Transitioning from an EU member state to an "outsider," the post-Brexit U.K. will be subject to EU scrutiny over whether its laws continue to comply with EU data privacy restrictions.[179] Depending on which EU laws or rules the U.K. decides to codify and keep,[180] U.K. law on data privacy will either be deemed "adequate," or inadequate and in need of data transfer agreements to make up the difference.[181] On the one hand, then, it may therefore be advisable for the U.K. to maximize their adoption of EU laws to ensure continued compliance with the GDPR.[182] The closer U.K. laws come to aligning to the GDPR requirements, the more likely its laws are to be deemed "adequate." On the other hand, a major motivator for Brexit in the first place was the desire to regain parliamentary sovereignty and "avoid EU regulation."[183]

These two positions highlight a core debate as the U.K. negotiates with the EU: whether to have a "soft" or a "hard" Brexit. The former refers to a compromise whereby the U.K. would have access to the European single market and would abide by European rules applicable to the single market.[184] The soft Brexit approach allows for reduced EU control, but maintaining a "quasi-EU member" status would come at the expense of the U.K. in that it

---

[178] Hunt & Wheeler, *supra* note 172 ("Former Foreign Secretary Philip Hammond, now Chancellor, wanted Britain to remain in the EU, and he has suggested it could take up to six years for the UK to complete exit negotiations.").

[179] *See* Callahan-Slaughter, *supra* note 3, at 246-47. For a discussion of the continued and enhanced adequacy scrutiny standard under the GDPR, see VILLENEUVE, ET AL., *supra* note 16 loc. F.5.(b) ("The GDPR maintains the general prohibition of data transfers to non-EU countries that are not officially recognized as "adequate" by the EU, and stricter conditions apply for obtaining certification of adequacy status.").

[180] *See* Sharp, *supra* note 5, at 2.

[181] *Cf.* Callahan-Slaughter, *supra* note 3, at 246-47, 251-52.

[182] Sharp, *supra* note 5, at 3.

[183] *Id.*

[184] *How a Soft Brexit Differs From a Hard One*, THE ECONOMIST (June 25, 2018), https://www.economist.com/the-economist-explains/2018/06/25/how-a-soft-brexit-differs-from-a-hard-one.

would lose the right to participate in passing EU law.[185] Since a soft Brexit would allow the U.K. to remain a part of either or both the Customs Union and EU single market, it would cause minimal trade disruptions but it would restrict the U.K.'s ability to enter into separate free trade agreements.[186]

The latter position, prioritizing regaining parliamentary sovereignty and the ability to self-regulate without EU interference, is more of a "hard Brexit" approach. A hard Brexit will be more disruptive of trade, especially European trade and especially in the short term; however, proponents of a hard Brexit argue that the upside will outweigh short-term deficits, as the U.K. will be free to negotiate free trade agreements elsewhere around the world on their own terms.[187]

Reports indicate that Prime Minister Theresa May favors a hard Brexit approach,[188] though she has also made assurances to during negotiations that the U.K. "will continue to be bound by all EU rules," which aligns closer to a soft Brexit.[189] Other government statements on its Brexit position as of summer 2018 proposes a mixed approach: a soft Brexit for goods, and a hard Brexit for services, coupled with a "facilitated customs arrangement".[190] The

---

[185] Georgina Downer, *The Choice Between Hard or Soft Brexit*, THE INTERPRETER (Mar. 8, 2018), https://www.lowyinstitute.org/the-interpreter/choice-between-hard-or-soft-brexit.

[186] *See id.*; *How a Soft Brexit Differs From a Hard One*, *supra* note 184.

[187] *How a Soft Brexit Differs From a Hard One*, *supra* note 184.

[188] *See, e.g.*, Annabelle Dickson, *Theresa May: No-Deal Brexit Preferable to EU Offer*, POLITICO (Sept. 26, 2018), https://www.politico.eu/article/theresa-may-no-deal-brexit-preferable-to-eu-offer/; John Grace, *Theresa May's Latest Brexit Speech Shows All Bets Are Off*, THE GUARDIAN (Mar. 2, 2018), https://www.theguardian.com/politics/2018/mar/02/theresa-may-brexit-speech-john-crace; Tara John, *What Exactly is a "Hard Brexit," Anyway?*, TIME (Jan. 17, 2017), http://time.com/4635762/theresa-may-hard-brexit-britain/; Adam Payne, Adam Bienkov & Thomas Colson, *Theresa May Tells Brexit Supporters to Face Up to "Hard Facts" About Leaving the EU*, BUSINESS INSIDER (Mar. 2, 2018);

[189] *How a Soft Brexit Differs From a Hard One*, *supra* note 184.

[190] *See* Ilia Roubanis, *May Proposes a Soft Brexit on Goods and a Hard Brexit on Services*, NEW EUROPE (July 13, 2018), https://www.neweurope.eu/article/may-proposes-soft-brexit-goods-hard-brexit-services/. For more on this position, also called the "Chequers Plan," see THE FUTURE RELATIONSHIP BETWEEN THE

final government position remains to be seen, but will surely have an impact on how the U.K. structures its trade deals—and, necessarily, also its data transfer deals—with the EU.

In addition to what type of exit the U.K. may have, another consideration is the sheer novelty of exiting the EU on its own. It is not clear what standard U.K. law will have to meet following its exit from the EU.[191] One possibility is that the EU will react more harshly in considering the U.K. law's "adequacy" simply because it is no longer a member state. Even if not directly in retaliation for leaving, it is possible that, because EU member states are not scrutinized in the same way as non-EU nations when seeking data transfers, provisions that were once benign as a member state will threaten the U.K.'s data privacy adequacy as a non-member.[192] An assumption of the EU adequacy principle is that EU member states inherently meet the adequacy standards, because member states are all subject to overarching EU laws governing member activities.[193] However, this is not necessarily the case. In fact, the *Tele2 Sverige AB v. The Swedish Post and Telecom Authority* case from January 2017 provides a critical example of laws, which had been in effect in EU member states for some time prior the CJEU ruling, that would otherwise have been "inadequate" to comply with EU law.[194] Therefore, in the wake of so much uncertainty, mapping out potential outcomes of U.K.-EU exit negotiations is important for anticipating the Brexit ripple effects, including its impact on data transfer agreements.

Managing the degree of uncertainty moving forward is important, in part, because of the implications that Brexit negotiations will have on U.K. industries.[195] The U.K. has held a

---

UNITED KINGDON AND THE EUROPEAN UNION, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/725288/The_future_relationship_between_the_United_Kingdom_and_the_European_Union.pdf (last visited Oct. 1, 2018).

[191] *See* Sharp, *supra* note 5, at 3.

[192] *See* Callahan-Slaughter, *supra* note 3, at 246-47, 251-52.

[193] *See* Sharp, *supra* note 5, at 3.

[194] *See* Gardner, *supra* note 160.

[195] Sharp, *supra* note 5, at 1, 3-4.

strategic position for many businesses from around the globe.[196] The services industry dominates the U.K. economy, accounting for 79% of its GDP in 2017.[197] In addition to its role as a data hosting hub in its own right,[198] these industries—including the U.K.'s largest sector, the financial services industry—generate massive amounts of data that is controlled and processed in the U.K.[199] Multinational organizations will have their eyes on U.K.-EU negotiations to evaluate the continued strategic value of doing business in—and, by extension, storing and managing their data in—the U.K.[200] Losing its status as the bridge to EU operations would be a heavy blow to the U.K. market.[201] This is especially true, as the U.K. economy has already been feeling negative ramifications since the Brexit referendum to leave the EU.[202] Already, neighboring Ireland has emerged as an attractive alternative to the U.K;[203] Germany and France are other potential challengers and attractive options for organization relocation.[204] It would seem likely, then, that the U.K. would prioritize policies for economic growth and recovery, which

---

[196] *See* Caitlin Morrison, *The Brexit Effect: How the Last Two Years Have Impacted the Economy*, INDEPENDENT (June 23, 2018), https://www.independent.co.uk/news/business/analysis-and-features/brexit-vote-two-years-eu-referendum-uk-economy-pound-sterling-gbp-usd-ftse-skills-shortage-a8410596.html.

[197] HOUSE OF COMMONS BRIEFING PAPERS, COMPONENTS OF GDP: KEY ECONOMIC INDICATORS, SN02787 (Sept. 10, 2018), https://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN02787#fullreport.

[198] Sharp, *supra* note 5, at 3.

[199] *See* PARLIAMENTARY OFFICE OF SCIENCE &TECHNOLOGY POST NOTE 'BIG DATA IN BUSINESS' NUMBER 469 (July 2014), http://researchbriefings.files.parliament.uk/documents/POSTPN-469/POST-PN-469.pdf.

[200] Sharp, *supra* note 5, at 3.

[201] Hunt & Wheeler, *supra* note 172.

[202] *See, e.g.*, Chris Giles, *What Are the Economic Effects of Brexit So Far?*, FINANCIAL TIMES (June 23, 2018), https://www.ft.com/content/dfafc806-762d-11e8-a8c4-408cfba4327c; Caitlin Morrison, *supra* note 189.

[203] Sharp, *supra* note 5, at 3.

[204] *Id.* at 4.

means, in part, maintaining its "strategic position for hosting data" for its various industries.[205]

One possibility for achieving this objective is to strike a Privacy Shield-like data transfer agreement between the U.K. and EU, which may be possible regardless of whether the U.K. seeks a hard or soft Brexit.[206] A data transfer agreement, however, would carry its own challenges, like the practicality of implementing such a large-scale transnational agreement while negotiating the massive amount of regulation necessary to leave the EU, and of updating the U.K. infrastructure to meet the demands of such a framework.[207] Furthermore, as the U.S. example shows, developing an agreement is only half the battle; the U.K. will have to demonstrate its enforcement of the agreement moving forward and continue to update the agreement as privacy rules in the EU evolve.

Scholars and commentators have also proposed modeling a new solution after agreements or organizations already in existence, including: (1) the European Economic Area, which allows for participation in the EU internal market and the free movement of goods, services, people, and capital; (2) the European Free Trade Association, through which the U.K. can "negotiation a bilateral trade agreement" with the EU for data transfers; and (3) negotiating an independent agreement under the aegis of the World Trade Organization.[208] Some of these options have been exercised by other non-EU countries with success. For example, Norway participates in the European Economic Area, and Switzerland has signed onto the European Free Trade Agreement.[209] These agreements clearly fall on the side of a soft Brexit, and, so far, the U.K. has not demonstrated clear interest in pursuing any of these alternative agreements. The U.K. has, however, been pursuing other transnational data agreement options to potentially increase trade on the other side of the pond with the U.S.

---

[205] *See id.* at 3-4.
[206] *Id.* at 4.
[207] *Id.*
[208] *Id.*
[209] *See, e.g.*, Privacy Shield Update, *supra* note 48.

IV. FORGING AN ALLIANCE? U.S.-U.K. DATA AGREEMENTS

The U.K.'s upcoming exit from the EU opens up the possibility of U.S.-U.K. agreements, outside the traditional constraints of EU regulations.[210] The U.K. has already signaled, in a publication outlining its "Brexit strategy," that it considers the U.S. its "single biggest export market" and prime target for a bilateral trade deal.[211] Any trade deal between the U.S. and the U.K. would be stalled, however, until the U.K.'s official exit from the EU.[212] Nevertheless, it would be in the interest of both the U.S. and the U.K. to continue to investigate the nature of a potential trade deal, both to improve each country's bargaining power with the EU and also as a "Plan B" to improve their global market options should negotiations with the EU fail to produce workable agreements for either the U.S. or the U.K.[213]

One of the reasons why the EU has been successful in forcing other nations to comply with its heightened data privacy protections is the EU's considerable market power.[214] Commentators have noted that, when calculating relative market strength, the U.S. market share is larger than the EU's, once the U.K. market is removed from the EU's side of the equation.[215] This means that Brexit, and especially a U.S.-U.K. trade agreement, could mark a powerful shift in which nations, or bloc of nations, carry the strongest global market power.[216] As a new market bloc, then, a

---

[210] Zeigler, et al., *supra* note 171, at 4.

211 The United Kingdom's Exit From and New Partnership with the European Union, 2017, Cm. 9417 (UK), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191
The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf.

[212] Zeigler, et al., *supra* note 171, at 4

[213] *See id.*

[214] Callahan-Slaughter, *supra* note 3, at 240 (citing Gregory Shaffer, *Globalization and Social Protection: The Impact of the EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 39 (2000)).

[215] Zeigler, et al., *supra* note 171, at 4.

[216] *See id.*

U.S.-U.K. alliance may gain an edge in negotiations with the EU, capable of coercing the EU into accepting terms more favorable to the U.S. and U.K.[217]

Likewise, because of the challenges presented to the U.S. and the U.K., independently, in striking a data transfer agreement with the EU, a U.S.-U.K. agreement would serve as an important safety net in case no workable solution with the EU can be reached.[218] Having a strong "Plan B," in the form of a "high-octane trade deal" between the U.S. and U.K. provides greater market security.[219] One downside to U.S.-U.K. trade agreements is that the two countries have similar strengths within the same industries; for example, both the U.S. and U.K. markets maintain strong finance and service sectors.[220] On the other hand, several factors, such as shared use of the English language, advantageous trading time-zones, relatively low taxes, reputable higher education and university systems, and respected legal systems with a shared common law background, make for a favorable U.S.-U.K. economic alliance.[221]

While a U.S.-U.K. trade deal is likely years in the future, the potential for a free trade deal is "highly likely."[222] As such, the free flow of trade would necessitate a strong data transfer agreement between the two countries to maximize business interactions.[223] This is especially true given the nature of the data that would be

---

[217] *See id.* ("It is much in the UK's interest to pursue these negotiations as diligently and as publically as possible. It will equally be in President Trump's interest to do all he can to strengthen the UK's position in these matters lest the UK be forced to accept terms from the EU that are not in either party's interest.").
[218] *See id.; see also*, Tim Ross, *U.K. Eyes Wall Street Access in Post-Brexit U.S. Trade Deal*, BLOOMBERG POLITICS (Apr. 13, 2017), https://www.bloomberg.com/politics/articles/2017-04-13/u-k-eyes-wall-street-access-in-post-brexit-u-s-trade-deal.
[219] Zeigler, *supra* note 171, at 4.
[220] *See* Ross, *supra* note 218; *Zeigler*, *supra* note 171, at 4.
[221] *See* Ross, *supra* note 218.
[222] Tom Welsh, *What a Post-Brexit Free Trade Deal Between the US and UK Could Mean for London*, CITY A.M. (Mar. 31, 2017), http://www.cityam.com/262054/post-brexit-free-trade-deal-between-us-and-uk-could-mean.
[223] Callahan-Slaughter, *supra* note 3, at 239-40.

implicated in the target markets, like financial services, legal services, and even data services themselves.[224] A potential agreement between the U.S. and U.K. would therefore likely involve "mutual recognition of data protection standards, and procurement" opportunities.[225]

The exact nature of the U.S.-U.K. agreement is presently speculative, because an agreement would not be possible before March 29, 2019 (the end of the two year period after invoking Article 50, assuming there is no extension to continue exit negotiations), and because negotiations between the U.S. and U.K. are neither in progress nor formally planned.[226] The future of a U.S.-U.K. agreement is likely to be shaped by U.K.-EU negotiations as well.[227] Unfortunately, the U.K. position entering into the U.K.-EU negotiations is far from clear or consistent. The U.K. Minister responsible for data protection has confirmed that the U.K. continues to support the GDPR and that the U.K. plans to comply with the GDPR.[228] Other Top U.K. officials, however, have indicated that they will press for a favorable Brexit deal. Prime Minister May has said that she is willing to walk away from exit negotiations without a new trade pact, and International Trade Secretary Fox has similarly indicated that the U.K. will not accept a Brexit deal "at any price."[229]

Therefore, while the current U.K. position is favoring EU regulatory compliance with the GDPR, the possibility that the U.K. will deviate from this position either as a matter of policy (i.e., the principle of separating itself from EU regulations) or to gain bargaining leverage in the greater context of exit negotiations still

---

[224] Welsh, *supra* note 222.
[225] *Id.*
[226] *See id.*
[227] *Id.*
[228] *UK Government Quizzed on GDPR Implementation and Post-Brexit Data Protection*, HUNTON & WILLIAMS: PRIVACY & INFORMATION SECURITY LAW BLOG (Feb. 3, 2017), https://www.huntonprivacyblog.com/2017/02/03/uk-government-quizzed-gdpr-implementation-post-brexit-data-protection/.
[229] Welsh, *supra* note 222.

exists.[230] This leaves sufficient room for U.K.-U.S. data transfer agreements to grow either alongside of or in lieu of the U.K.-EU agreements, depending on how exit negotiations develop in the coming years.

CONCLUSION

Between the pending challenge to the Privacy Shield, Brexit, and the GDPR, the data transfer agreements and relationships between the U.S., U.K., and EU will most likely all need to be renegotiated in the near future.[231] With so much potential change on the horizon between three major actors in the data management and processing sector, both the individual terms of data transfer agreements and the balance of international market power are up for grabs.[232]

The current U.S.-EU agreement, the Privacy Shield, rests on thin ice. Between legal challenges in EU courts and heightened GDPR standards, the Privacy Shield will likely be inadequate to comply with the EU data privacy requirements in the near future.[233] While the EU has maintained strong, coercive market power sufficient to press non-EU nations, like the U.S., to accept and comply with heightened data privacy standards, international market power dynamics are poised to shift following Brexit.[234] In negotiating a new agreement, the U.S. may be able to use its relatively strengthened position, compared to an EU without the added U.K. market force, to negotiate for more favorable, less restrictive data privacy terms that are consistent with the U.S. regulatory framework.[235]

Brexit may also independently necessitate data transfer agreements with either or both the EU and the U.S. Though the U.K. has maintained support of the GDPR, it is unclear what the terms of

---

[230] *See id.*
[231] *See supra* Part II-IV.
[232] *See id.*
[233] *See* Goldstein, *supra* note 1, at 21.
[234] *See* Callahan-Slaughter, *supra* note 3, at 240; Zeigler, *supra* note 171.
[235] Zeigler, *supra* note 171, at 4.

EU exit negotiations will be, whether the EU will continue to recognize U.K. law (even if it adopts and complies with the GDPR regulations) as "adequate," and what a potential data transfer agreement between the EU and U.K. would look like moving forward after exit negotiations wrap up.[236] But the EU is not the only major player with whom the U.K. is courting trade negotiations; the U.K. has also indicated that the U.S. is a prime target for trade deals, and U.S.-U.K. data transfer and trade agreements would be advantageous both in its own right and as a bargaining tool in EU negotiations for both countries.[237]

While the large degree of uncertainty, especially when it comes to the U.K.'s next moves, means many of this paper's predictions for the future of multinational data transfer agreements are speculative, mapping out the possibilities is nonetheless helpful to predict best-case and worst-case scenarios. It seems, currently, that the worst case scenario would be a retreat to isolationism, regardless of the implications for EU data transfer restriction regulation compliance, because it would impede global trade opportunities and international communications.[238] Though this approach would possibly hinder the flow of data, technology, and information, it would protect national interests in gaining access to data in the event that data transfer agreements continue to be invalidated and negotiations for replacement agreements break down.[239] Once again, the looming threat of data isolationism can, if nothing else, impress upon negotiating parties the importance of reaching a workable data transfer solution.[240]

With great uncertainty comes great opportunity. While having to renegotiate up to three major data transfer agreements in the next few years will be practically challenging, it can provide a blank slate to reconcile core differences in privacy objectives and approaches. Building new data privacy arrangements between three major

---

[236] *See supra* Part III.
[237] *See supra* Part IV.
[238] *See supra* Part II.D.
[239] *See id.*
[240] *See id.*

international players is an opening to broaden multinational data transfer agreements into a workable, uniform, global data regime.