Privacy and/or Trade

Anupam Chander† *& Paul Schwartz*††

International privacy and trade law developed together but are now engaged in significant conflict. Current efforts to reconcile the two are likely to fail, and the result for globalization favors the largest international companies able to navigate the regulatory thicket. In a landmark finding, this Article shows that more than sixty countries outside the European Union are now evaluating whether foreign countries have privacy laws that are adequate to receive personal data. This core test for deciding on the permissibility of global data exchanges is currently applied in a nonuniform fashion with ominous results for the data flows that power trade today.

The promise of a global internet, with access for all, including companies from the Global South, is increasingly remote. This Article uncovers the forgotten and fateful history of the international regulation of privacy and trade that led to our current crisis and evaluates possible solutions to the current conflict. It proposes a Global Agreement on Privacy that would be enforced within the trade order, but with external data-privacy experts developing the treaty's substantive norms.

† Scott K. Ginsburg Professor of Law and Technology, Georgetown University.

†† Jefferson E. Peyser Professor, U.C. Berkeley School of Law. For their helpful suggestions on previous drafts, we would like to thank Kathleen Claussen, Jill Goldenziel, Sylvia Lu, Indra Spieker, Lior Strahilevitz, and David Vladeck. We are grateful to a dream team of research assistants at Berkeley and Georgetown: Shayanna Ahuja, María José Badillo, Ryan Campbell, Robert Fairbanks, Gabriela Gabbidon, Saabhir Gill, Kiana Harkema, Joey Kingerski, Leo Koepp, Meet Mehta, Emma Neukrug, Sudipt Parth, Rishi Ray, Sophia Wallach, and Andy Zachrich. For superb editing, we thank Ian Howard and his colleagues on the *University of Chicago Law Review*. This Article is dedicated to the memory of Professor Joel R. Reidenberg, a great figure in privacy law and a cherished friend.

INTRODUCTION

Privacy and trade appear to be in a mortal contest. Will trade be the death of data privacy, as international flows of personal information across the world place our privacy at risk? Or will data privacy be the death of trade, as restrictions on information flows make modern trade increasingly difficult?

Countries across the world are now creating barriers to personal data traveling across borders and raising threats to the mutual dependence of privacy and trade.[1] In addition, decisions of the highest court in the European Union, the European Court of Justice, have greatly complicated transfers of personal data outside the European Union.[2] In the wake of these judgments, European authorities have questioned—or, in certain cases even

---

[1] *See, e.g.*, Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, 169 PRIV. L. & BUS. INT'L REP. 1, 1 (2021) [hereinafter Greenleaf, *Global Data Privacy Laws 2021*] (noting a 10% increase in the number of countries with a data privacy law from 2019–20).

[2] *See, e.g.*, Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, ECLI:EU:C:2020:559, at 30 (July 16, 2020) [hereinafter *Schrems II*]; *see also* Case C-362/14, Schrems v. Data Prot. Comm'r, ELCI:EU:C:2015:650, at 21 (Oct. 6, 2015) [hereinafter *Schrems I*].

banned—the use of U.S.-based technology because these products transfer personal data to the United States. The decisions implicate Microsoft Office, Amazon Web Services, Cloudflare, MailChimp, and, most recently, Google Analytics.[3] LinkedIn remains banned in Russia because it refuses to store user data in that country.[4]

Cross-border transfers of personal information are now the lifeblood of modern trade, but those exchanges are increasingly imperiled.[5] Moreover, privacy regulations implicate not just services but modern goods as well. A Mercedes car now contains some one hundred million lines of code, one hundred electronic control units, and ten operating systems.[6] Tesla stores the data produced by its Chinese cars in that jurisdiction to comply with national data localization regulations.[7] Even toothbrushes and dolls can be connected to the internet.[8] Trade in goods and services alike now requires cross-border data flows. While the addition of intellectual property to the trade regime has received a great deal of recent attention, there has been less awareness of

---

3 European authorities have opened an inquiry into the use of Amazon Web Services and Microsoft Office 365 by public institutions. *The EDPS Opens Two Investigations Following the "*Schrems II*" Judgment*, EUR. DATA PROT. SUPERVISOR (May 27, 2021), https://perma.cc/A48K-3S5X. The U.S.-based cybersecurity company Cloudfare has been barred from use in the Portuguese national census. *CNPD, Deliberação/2021/533, (Deliberation)*, GDPRHUB (Apr. 28, 2021), https://perma.cc/MN65-N68C. The Bavarian Data Protection Authority has ruled that using Mailchimp newsletters might violate data protection law. *See Bavarian DPA (BayLDA) Calls for German Company to Cease the Use of "Mailchimp" Tool*, EUR. DATA PROT. BD. (Mar. 30, 2021), https://perma.cc/DSU7-UV55. Google Analytics has been found to violate data protection law by authorities in Austria and France because it transfers personal data to the United States. Datenschutzbehörde, Teilbescheid Spruch [Partial Decision] (Dec. 22, 2021), https://perma.cc/AYA4-4UYE; *Use of Google Analytics and Data Transfers to the United States: The CNIL Orders a Website Manager/Operator to Comply*, CNIL (Feb. 10, 2022), https://perma.cc/7FUT-SGKC; Matt Burgess, *Europe's Move Against Google Analytics is Just the Beginning*, WIRED (Jan. 19, 2022), https://perma.cc/RRU6-LKZP.

4 Alexander Winning & Maria Kiselyova, *LinkedIn Fails to Agree with Russia on Restoring Access to Site*, REUTERS (May 7, 2017), https://perma.cc/9FZW-ARDH.

5 As Matt Burgess at *Wired* concisely sums up, "European regulators [ ] don't like the way US tech companies send data across the Atlantic." Burgess, *supra* note 3.

6 Lucian Cernat, *The (Cyber) Security of Global Supply Chains: Is This a Blind Spot for Industry 4.0?*, EUR. CTR. FOR INT'L POL. ECON. (Oct. 2021), https://perma.cc/PM9R-X5KP (describing a Mercedes S-class).

7 James Vincent, *Tesla Will Store Chinese Car Data Locally, Following Government Fears About Spying*, THE VERGE (May 26, 2021), https://perma.cc/4JPV-G6XC.

8 Benny Evangelista, *Smart Toothbrushes the Latest Internet of Things Battleground*, SFGATE (June 9, 2016), https://perma.cc/SE5M-L3AP (noting that the brush provides "a three-dimensional map of the user's teeth"); Philip Oltermann, *German Parents Told to Destroy Doll That Can Spy on Children*, THE GUARDIAN (Feb. 17, 2017), https://perma.cc/5LRD-7UL5.

the trade law that regulates services, even though it governs the principal economic activity of developed nations and, increasingly, developing nations.[9]

Early scholarship recognized the critical role of privacy in international trade. In 1999, Professor Joel Reidenberg called for a "General Agreement on Information Privacy" to sit alongside the General Agreement on Tariffs and Trade and the General Agreement on Trade in Services.[10] In 2002, Professor Gregory Shaffer found hope for a reconciliation between privacy and trade through mutual recognition systems.[11] Yet, today, some scholars would exempt privacy measures from trade law almost entirely, arguing that, as a fundamental right, privacy should not be subject to disciplines that liberalize trade. For example, Professor Kristina Irion, Dr. Svetlana Yakovleva, and Professor Marija Bartl have proposed to "fully exempt[ ] the existing and future EU legal framework for the protection of personal data" from the scope of future EU trade treaties.[12] Indeed, in its trade negotiations, the European Union seeks a blanket exemption for "safeguards it deems appropriate to ensure the protection of personal data and privacy."[13] In short, the European Union today seeks to

---

9 In 2021, for example, U.S. personal consumption of services ($10 trillion) was double that of goods ($5 trillion). U.S. BUREAU OF ECON. ANALYSIS, TABLE 2.3.5U. PERSONAL CONSUMPTION EXPENDITURES BY MAJOR TYPE OF PRODUCT AND BY MAJOR FUNCTION (Aug. 25, 2022), https://perma.cc/C5XR-8X33.

10 Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1359–62 (2000) [hereinafter Reidenberg, *Resolving*]. Two years later, Reidenberg announced that "an international treaty is likely the only sustainable solution for long-term growth in trans-border commercial interchange." Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 719 (2001) [hereinafter Reidenberg, *E-Commerce*].

11 Gregory Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29, 67–69 (2002) (discussing the Safe Harbor program as an example of a mutual recognition system working to balance the interests of trade liberalization and the protection of individuals' privacy).

12 Kristina Irion, Svetlana Yakovleva, & Marija Bartl, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements*, INST. FOR INFO. L., UNIV. OF AMSTERDAM 1, 22 (2016), https://perma.cc/Y3YZ-KKUC [hereinafter Irion et al., *Trade and Privacy*]. For other scholarship with this perspective, see Svetlana Yakovleva & Kristina Irion, *Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, 10 INT'L DATA PRIV. L. 201, 218 (2020) [hereinafter Yakovleva & Irion, *Pitching Trade*]; Svetlana Yakovleva & Kristina Irion, *The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection*, 2 EUR. DATA PROT. L. REV. 191, 208 (2016).

13 Eur. Comm'n, *Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)* art. B.2 (May 2018), https://perma.cc/432N-JWZS.

ensure that trade rules can never be used to question any action that it declares to be promotive of privacy.

This Article shows that data privacy law and contemporary international trade law were created simultaneously and in contemplation of the other.[14] But in taking the historic step in 1994 of creating the General Agreement on Trade in Services (GATS), governments also crafted an open-ended, yet cabined, privacy exception in this treaty.[15] GATS neither establishes global minimum standards for privacy nor provides an international process for creating such standards. It simply allows signatory nations to protect privacy so long as this action can be said to be "necessary."[16] This Article terms this nonresolution, this exception for necessary privacy protections, the "Privacy Bracket."[17]

The result has been a regulatory thicket of divergent privacy rules inconsistently applied.[18] The harm is to the promise of an internet that would permit workers in the Global South to provide services and goods to consumers and businesses in the Global North. Ever-increasing privacy hurdles run the risk of restricting the provision of higher-value information-based business to the Global North.

The current global regulation of privacy and trade has reached a crisis point. In response, this Article proposes a Global Privacy Agreement, a new treaty, and one (like GATS) to be anchored within the World Trade Organization. As her term ended in 2021, outgoing UK Privacy Commissioner Elizabeth Denham called for a "Bretton Woods [Conference] for data."[19] In 1944, the Bretton Woods Agreement established the modern basis of the international economic order.[20] This Article takes up Commissioner Denham's call and offers a regime for harmonizing data privacy and trade.

---

14 *See infra* Part I.A.3.

15 General Agreement on Trade in Services art. XIV(c)(ii), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 (1994) [hereinafter GATS].

16 *Id.*

17 *See infra* Part I.A.1.

18 *See infra* Part I.B.2.

19 Elizabeth Denham, *Solving the Billion-Dollar Question: How Do We Build on the Foundations of Convergence?*, GLOB. PRIV. ASSEMBLY (Nov. 1, 2021), https://perma.cc/Q9UW-ZU68.

20 Isaac O.C. Igwe, *History of the International Economy: The Bretton Woods System and Its Impact on the Economic Development of Developing Countries*, 4 ATHENS J.L. 105, 111–12 (2018).

Our argument unfolds in three steps. Part I first uncovers the forgotten shared history of data privacy and international trade law that led to GATS.[21] It reveals that the tension between privacy and trade was part of the raison d'être for this pathbreaking trade agreement.[22] Both the United States and the European Union worried that their trade in services would be blocked by data-flow restrictions in other countries, and thus sought the expansion of international trade rules to govern services. Beginning at this time, the European Union also created Europe-wide data protection law so that national privacy rules in its member states would not become a stumbling block to intra-European trade.[23] Yet, at the same time, it proposed, and the U.S. agreed to, the Privacy Bracket, which set the stage for the current threat to cross-border trade.

Part I then turns to the reckoning, the crisis in international data flows, which is driven by developments in global data privacy law.[24] Almost all of the discussions of "adequacy," a core feature of global data privacy, focus on how the European Union determines whether a foreign jurisdiction's data protection law meets this standard.[25] Yet, in a major empirical finding, this Article identifies the creation of adequacy standards in sixty-one countries *outside* the European Union.[26] This little-explored phenomenon is part of a larger development: the splintering of data-privacy standards. The result is widely divergent requirements for data-transferring entities, which increase compliance costs and limit hopes of a new global distribution of economic opportunities.

Part II examines the models that nations have developed to solve the privacy-or-trade conundrum. The first model, which is associated with the United States, favors trade over privacy.[27] It proceeds through the development of free trade agreements strictly limiting data-privacy measures that might conflict with

---

21 *See infra* Part I.A.2.

22 *See infra* Part I.A.2.

23 For a discussion, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 480–83 (1995).

24 *See infra* Part I.B.

25 This perspective was displayed most recently in coverage of the post-Brexit UK-EU adequacy discussions. Daphne Leprince-Ringuet, *A Major International Data Flow Problem Just Got Resolved. But Another Row Is Already Brewing*, ZDNET (June 22, 2021), https://www.zdnet.com/article/a-major-international-data-flow-problem-just-got-resolved-but-another-row-is-already-brewing/.

26 *See infra* Part I.B.1 and Appendix A.

27 *See infra* Part II.A.

free data flows. The second model, one favored by the European Union, promotes data privacy over trade.[28] Finally, the third model, one accepted by both the United States and European Union, establishes accountability mechanisms that permit entities to opt into privacy protections for international data flows.[29] This Article's innovative taxonomy leads to a remarkable conclusion, which is that both the United States and European Union have converged on the need for an escape valve—that is, a mechanism to prevent a ruinous blockage in the world's data flows.[30]

Part III turns to solutions. It identifies underlying normative considerations underlying global trade and data privacy. In a correction to current scholarship, it argues that both privacy and trade share important values.[31] The global trade regime seeks more than neoliberal market optimization. Trade law can also promote the global democratization of opportunity. As for privacy, its values include self-determination and democratic community. Part III then explores three possible solutions to the crisis: "muddling through" within the current policy framework;[32] heightening enforcement cooperation through a new Global Privacy Enforcement Treaty;[33] and, finally, a new substantive Global Privacy Agreement.[34] We champion the last approach but explore the virtues and drawbacks associated with each solution.

Finally, a few words about terminology. For conceptual clarity, this Article employs three related but distinct terms: "data protection," "information privacy," and "data privacy." "Data protection" is the accepted, standard term applied to Europe's body of law concerning the processing, collection, and transfer of personal data.[35] It is also the favored term in most countries outside the United States, even in common law nations such as the United Kingdom.[36] Although U.S. law lacks such a uniformly accepted single term, it tends to rely on the expression "information

---

28 *See infra* Part II.B.

29 *See infra* Part II.C.

30 *See id.*

31 *See infra* Part III.A.

32 *See infra* Part III.B.

33 *See infra* Part III.C.

34 *See infra* Part III.D.

35 *See* Paul M. Schwartz, *The Data Privacy Law of Brexit: Theories of Preference Change*, 22 THEORETICAL INQUIRIES L. 111, 112–13 (2021); *see also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 121–22 (2017).

36 For example, a leading treatise on U.K. data protection law is ROSEMARY JAY, DATA PROTECTION LAW AND PRACTICE (5th ed. 2020).

privacy."[37] When this Article discusses the concept to refer to the area generally, this Article uses the terms "data privacy" or "privacy."

I. THE BRACKETING AND THE RECKONING

Data privacy law and international trade law, as we know them today, came into their own in the early 1990s. While each had earlier incarnations, they went global together. This Part tells the story of how the modern regimes of data privacy law and international trade law were created in full contemplation of each other. Nonetheless, the international trade regime ultimately chose to defer decision-making about privacy, and to allow it to remain the realm of individual nations, subject to certain limitations. The result has generated the current state of crisis for global data flows.

A. The Privacy Bracket

In 1994, the nations of the world finalized the new international trade order with the conclusion of the monumental Uruguay Round of multilateral negotiations.[38] This process established the World Trade Organization (WTO), which introduced, for the first time, services to the global trade rules, which had previously governed only goods.[39] With the General Agreement on Trade in Services (GATS), each signatory country committed to liberalize trade in certain specified services by agreeing to provide market access and equal treatment to suppliers from other WTO member states.[40] The goal was to ensure that countries would treat those suppliers as well as their own nationals and not play favorites among the other member states.[41] With the addition of services, the international trade order expanded its domain dramatically.

---

37 Hence, a leading casebook in this area in the United States is DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (7th ed. 2021).

38 David W. Leebron, *An Overview of the Uruguay Round Results*, 34 COLUM. J. TRANSNAT'L. L. 11, 11–12 (1996).

39 Bernard Hoekman, *The General Agreement on Trade in Services: Doomed to Fail? Does it Matter?* 8 J. INDUS. COMPETITION TRADE 295, 296 n.1 (2008).

40 *See* GATS, *supra* note 15, at arts. II (most-favored-nation treatment), XVI (market access), & XVII (national treatment).

41 *See The General Agreement on Trade in Services (GATS): Objectives, Coverage and Discipline*, WTO, https://perma.cc/P7YJ-CC9S.

GATS set up a comprehensive framework of coverage by extending both to services where the supplier is present within the territory of the member, and those where the supplier is remote.[42] The treaty's overarching goals are to create a stable climate for global trade and to promote competition and market liberalization, consistent with each nation's regulatory goals.[43]

1. The privacy bracket and its meaning.

How then would the new global trade order deal with data privacy? Some today might assume that privacy was not a significant concern in this pre-internet area, but the governments that negotiated GATS did recognize that trade in services implicated data privacy. Indeed, as this Part demonstrates, the issue of cross-border data flows has been on the global agenda since the 1980s along with an understanding that many of these flows involved personal information, and, hence, implicated privacy. Yet, the GATS negotiators in 1994 decided to largely exclude privacy laws from the new international trade regime for services.

GATS set out the Privacy Bracket as well as a number of other exceptions in Article XIV.[44] The exceptions permit member states to take measures that might otherwise violate the treaty—that is, to leave certain areas outside of the treaty's reach under certain conditions. These areas include the protection of public order and human health as well as the prevention of deceptive and fraudulent practices. As for the Privacy Bracket, Article XIV(c)(ii) contains the critical exception: "[N]othing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures . . . necessary to secure compliance with laws or regulations . . . including those relating to: *the protection of the privacy of individuals in relation to the processing and dissemination of personal data*."[45] The import of this language is clear: rather than establishing global minimum standards for privacy or developing an international process for the creation of such standards, the GATS agreement brackets the issue of privacy.

GATS did not simply create a privacy exception but also set limits on its scope. Like the other exceptions in Article XIV, GATS

---

42 *See* GATS, *supra* note 15, at art. I(2) (describing modes of supply).

43 *Id.* at preamble (discussing the motivations and goals regarding the act).

44 *Id.* at art. XIV.

45 *Id.* at art. XIV(c)(ii) (emphasis added).

sought to limit the possible misuse of its exclusion for privacy. For example, a signatory nation might claim to be regulating properly within an excluded area but might really be seeking to benefit one of its domestic industries. Hence, before the language quoted above, Article IV begins with a general limitation on all its exceptions by making them "[s]ubject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services."[46] The language of the privacy exclusion then adds a specific requirement that the adopted measure be "necessary" for the protection of data privacy.[47]

Rather than resolve the complications raised by the flow of personal data across borders, GATS decided in 1994 not to engage with the question of how best to protect privacy amid a growing global trade in personal data. By bracketing privacy, GATS deferred to the future the difficult decisions on when a privacy measure that restrains trade is necessary or discriminatory. At the same time, the Privacy Bracket has considerable built-in complexity and several weak points. Most crucially, it can be justified only under relatively stringent tests, though WTO tribunals have yet to police it. Restrictions made in the name of privacy must be "necessary" and cannot be unjustifiable or disguised discriminatory treatment. These issues merit exploration at this juncture.

First, a privacy restriction as well as the other exceptions in Article XIV must be "necessary." In nonprivacy contexts, the determination of whether such a restriction is necessary has been found to turn on whether a "reasonably available" alternative exists that achieves the same policy goals but is less trade restrictive.[48] Second, as the general limitation on all GATS exceptions states, the privacy restriction should not constitute "a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services."[49] As Professor Rolf Weber and Dr. Dominic Staiger

---

46 *Id.*

47 *See* GATS, *supra* note 15, at art. XIV(c)(ii).

48 Appellate Body Report, *United States—Measures Affecting The Cross-Border Supply of Gambling and Betting Services*, ¶¶ 304–05, 308, WTODoc. WT/DS285/AB/R (adopted Apr. 7, 2005) (determining necessity under Article XIV(a) in nonprivacy contexts).

49 GATS, *supra* note 15, at art. XIV.

have observed, such a demonstration of nondiscrimination demands "consistency of enforcement."[50] For example, this test would require that a GATS signatory did not single out one state for tougher application of extraterritorial provisions found in its data privacy law. Thus, the privacy exception is limited by a requirement that it not be disguised protectionism or favoritism.

Third, and surprisingly, the bounds of the Privacy Bracket have remained untested since its creation in 1995. There is a process for nations to complain about misuse of Article XIV(c)(ii), which would be through the WTO's Dispute Settlement Understanding.[51] While many countries, including the United States, have brought claims about violations of services trade commitments, no country has yet sought to test a potentially discriminatory use of the Privacy Bracket. Were a privacy law to be contested, the scholarship agrees that a WTO Tribunal would be obliged to use a "holistic necessity analysis through a 'weighing and balancing' test."[52] But, as Dr. Neha Mishra pointed out, there is "no international consensus" on the proper range of "tools used to achieve cybersecurity/privacy."[53]

In contrast to this official inaction, leading scholars agree that today's data privacy laws and practices might well exceed the bounds of the Privacy Bracket. Scholars have, in particular, singled out EU data protection law as problematic. Irion, Yakovleva, and Bartl argued, "Demonstrating the required 'consistency of enforcement' could be a challenge for the EU, in particular with a view to administering and adopting adequacy decisions by the Commission."[54] In the assessment of Professor Mira Burri, "[I]t can well be maintained that there are less trade restrictive measures that are reasonably available for achieving the EU's desired level of data protection."[55] Recall that an ironclad requirement of Article XV for use of the Privacy Bracket is that the adopted measure be "necessary." If less trade-restrictive

---

50 ROLF H. WEBER & DOMINIC STAIGER, TRANSATLANTIC DATA PROTECTION IN PRACTICE 58 (2017).

51 *See* Marrakesh Agreement Establishing the World Trade Organization: Understanding on Rules and Procedures Governing the Settlement of Disputes, Annex 2, Article 1.1, Apr. 15, 1994, 1869 U.N.T.S. 401 ("The rules and procedures of this Understanding shall apply to disputes brought pursuant to the consultation and dispute settlement provisions of the agreements listed in Appendix I to this Understanding.").

52 Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19 WORLD TRADE REV. 341, 356 (2020).

53 *Id.* at 358.

54 Irion et al., *Trade and Privacy*, *supra* note 12, at 55.

55 Mira Burri, *Interfacing Privacy and Trade*, 53 CASE W. RSRV. J. INT'L L. 35, 66 (2021).

measures are available, the data-privacy measure in question is likely to be deemed to be disguised protectionism, and, hence, invalid under GATS. Finally, Professor Christopher Kuner observed that the European Union employs its test for judging the permissibility of international data transfers in part using political criteria.[56] In contrast, GATS requires an analysis based on objective factors in determining the permissibility of recourse to the Privacy Bracket.[57]

In sum, the existing approach to privacy in trade law strictly delimits the privacy exception within a demanding test for nondiscrimination and a required comparison of alternative, less trade-restrictive measures to promote privacy. However, these limitations of GATS Article XIV have yet to be invoked through dispute resolution. Instead, the Privacy Bracket opened the way for numerous countries to enact requirements limiting cross-border data flows from their territory. While GATS did not entirely disregard privacy, it pushed back to a later day any hard decisions and invited each nation to go its own way.

2. The prehistory of the bracket.

Having delineated the contours of the current resolution in GATS of possible conflicts between privacy and trade, this Article now describes the path to this decision. Today, it is commonplace to assume that international trade law failed to grapple with issues of privacy because cross-border data flows were largely unknown at the time of GATS.[58] Yet, the pre–Uruguay Round policy debate recognized that issues of privacy and trade were intertwined.

---

[56] Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, *in* REINVENTING DATA PROT. 263, 265–66 (Serge Gutwirth et al. eds., 2009). Kuner noted, for example, that the decision finding Argentina adequate "was ultimately approved because of politics." *Id.* at 265.

[57] *See, e.g.*, Mishra, *supra* note 52, at 350; Appellate Body Report, *supra* note 48, at ¶ 304 ("We note, at the outset, that the standard of 'necessity' provided for in the general exceptions provision in an *objective* standard." (emphasis in original)).

[58] *See, e.g.*, Mishra, *supra* note 52, at 350 ("Being a pre-internet era treaty, the provisions contained in GATS were not designed keeping in mind the public policy challenges of a digital era, particularly those related to cross-border data transfers via the internet."); Shane Tews, *Are Privacy Laws Compatible with International Trade? Highlights from My Conversation with Nigel Cory*, AEI (Sept. 14, 2021), https://www.aei.org/technology-and-innovation/are-privacy-laws-compatible-with-international-trade-highlights-from-my-conversation-with-nigel-cory/ ("The trade rules we have under the World Trade Organization are relics of the 19th century and are just not ready for today's digital 21st century.").

Before GATS, a wide range of commentators in multiple fora worried that foreign privacy laws might interfere with a free flow of information. For example, the U.S. House of Representatives held a hearing in 1980 on international data flows at which the Chairman of the Government Information and Individual Rights Subcommittee described "the protection of personal privacy" as a possible new "barrier[ ] to trade."[59] Two speakers at the hearing warned of a future balkanization of information laws, including a heighted burden on U.S. firms "having to meet the variegated requirements of different countries' laws and regulations."[60]

This awareness of a link between privacy and trade also led to the two leading first-generation international guidelines regarding data privacy. These are the *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (1980) of the Organisation for Economic Cooperation and Development (OECD)[61] and the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention 108) (1981) of the Council of Europe.[62]

Prior to these guidelines, the United States and Western Europe had been active in important policy discussions about data privacy that preceded the enactment of pioneering data privacy laws. An influential 1973 white paper from the U.S. Department of Health, Education, and Welfare (HEW) first identified elements of a code of so-called Fair Information Practices (FIPs).[63] The early statutes and the HEW paper demonstrate an emerging debate about an intellectual framework of best practices for the processing of personal data. The OECD Guidelines and the Council of Europe's Convention 108 also demonstrate that this global conversation about privacy protection had trade considerations in mind.

The OECD Privacy Guidelines of 1980 represent an important early "soft law" implementation of FIPs. The OECD is a

---

59 International Data Flow: Hearings Before a Subcomm. of the H. Comm. on Gov't Operations, 96th Cong. 1 (1980) (statement of Rep. Richardson Preyer, Chairman, Gov't Info. and Individual Rights Subcomm.).

60 *Id.* at 114 (statement of Robert E. Walker, Vice President, Cont'l Ill. Bank).

61 Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECDDoc. C(80)58/FINAL (adopted Sept. 22, 1980) [hereinafter OECD Guidelines], *amended by* OECDDoc. C(2013)79 (adopted July 10, 2013).

62 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 [hereinafter Convention 108].

63 U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS xx–xxiii (1973).

group of leading industrialized countries, including the United States, concerned with global economic and democratic development.[64] The OECD Guidelines are a nonbinding framework—that is, they are soft law, which Professors Andrew Guzman and Timothy Meyer defined as representing a "continuum" between "fully binding treaties and fully political positions."[65] The OECD Guidelines seek to influence policymaking by offering what Guzman and Meyer might call a "focal point for cooperation."[66] Indeed, the Guidelines have assisted nations by crafting a lingua franca for discussing data-privacy issues.

The OECD Guidelines seek more uniform treatment of personal data throughout the world in order to protect privacy as well as to keep personal data flowing globally. As the preface to the Guidelines declares, "[T]here is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers . . . caus[ing] serious disruption in important sectors of the economy, such as banking and insurance."[67] The Guidelines devote four sections to international transfers. Their cornerstone idea is to obligate OECD members to "take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure."[68] The Guidelines call for a state to "refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the reexport of such data would circumvent its domestic privacy legislation."[69]

Finally, the Guidelines seek to ensure proportionality in domestic privacy legislation. They state, "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed

---

64 For more about the OECD, see *Together, We Create Better Policies for Better Lives*, OECD, https://perma.cc/5GE3-FQJQ.

65 Andrew T. Guzman & Timothy L. Meyer, *International Soft Law*, 2 J.L. ANALYSIS 171, 173, 180 (2010) ("The central mystery of soft law is the fact that states opt for something more than complete absence of commitment, but something less than full-blown international law. This middle-of-the-road strategy is widely used in international law.").

66 *Id.* at 176.

67 OECD Guidelines, *supra* note 61, at Preface.

68 *Id.* at ¶ 16.

69 *Id.* at ¶ 17.

requirements for such protection."[70] Thus, already in 1980, we see the germ of a concept that later appears in GATS, which is to mandate the least trade-restrictive privacy measures available to cabin any use of privacy law as a form of disguised protectionism.

Further evidence of a linkage between privacy and trade is found in the Council of Europe's Convention 108. A separate organization from the European Union, the Council of Europe is the leading human rights organization of the continent, with forty-seven member states, including all twenty-seven EU members.[71] Convention 108 is an international treaty, which twenty-one countries had already acceded to by the mid-1990s when GATS was adopted.[72] Prior to the European Union's involvement in the area of data privacy, the Convention was the most important Europe-wide agreement regarding the processing of personal data.[73] It is a "non-self-executing" treaty, which means it requires signatory nations to enact domestic data protection legislation to give effect to its principles and to provide a common core of safeguards for personal data processing.[74] It draws on the kinds of FIPs developed in the HEW's White Paper of 1973 and present in pioneering European privacy laws in France, Germany, and Italy.[75]

Convention 108 also offers a solution to twin threats raised by international data flows: data havens and export licenses. The explanatory report for Convention 108 explained that some "data users might seek to avoid data protection controls by moving their operations, in whole or in part, to 'data havens,' i.e.[,] countries

---

70 *Id.* at ¶ 18.

71 *See Values: Human Rights, Democracy, Rule of Law*, COUNCIL OF EUR., https://perma.cc/7JKD-PBZY.

72 Treaty Office, *Chart of Signatures and Ratifications of Treaty 108*, COUNCIL OF EUR. PORTAL (Sept. 19, 2022), https://perma.cc/YDU7-ANQ9. By January 1995, when GATS came into force, fifteen countries had ratified Convention 108 and twenty-one countries had signed the Convention. *See id.*

73 Schwartz, *supra* note 23, at 477; COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 133–36 (1992).

74 Schwartz, *supra* note 23, at 477:

> The Convention is a "non-self-executing treaty"; its standards do not directly impose binding norms on signatory nations. However, it does require signatory nations to establish domestic data protection legislation that will both give effect to the Convention's principles and provide a common core of safeguards for the processing of personal information.

See also BENNETT, *supra* note 73, at 135.

75 Schwartz, *supra* note 23, at 477.

which have less strict data protection laws, or none at all."[76] Some countries might respond to the problem of data havens by demanding "a license for export" of data.[77] By committing to the Convention, countries could avoid a race to the bottom (the data haven) and obviate a need to hamper data trade (by imposing licenses for export).

Accordingly, Convention 108 requires free flows of data among signatory nations unless otherwise expressly provided.[78] The most important of its exceptions to its "free flow" rule applies to a signatory nation that has enacted "specific regulations for certain categories of personal data."[79] Under the Convention, signatory nations that provide these specific regulations, which are intended to protect sensitive information, are permitted to block data exports to another treaty party that lacks equivalent levels of protection.[80] While the Convention does not explicitly discuss transfers of personal data to nonsignatory nations, leading treatises of the era interpreted it as permitting restrictions on data transfers to lands without equivalent privacy standards.[81]

There is a final element in this pre-GATS landscape regarding international data transfers. By the mid-1980s, many national European data protection laws expressly permitted the blocking of international transfers of personal information.[82] Various approaches were taken at that time in Belgium, Denmark, France, Germany, Portugal, Spain, and the United Kingdom.[83] These included nations, such as Portugal and Spain, that explicitly set out an "equivalency" standard, and those, such as Belgium and France, that merely suggested that some international data transfers would be impermissible, including to other European nations.[84] Other countries, such as Denmark and the United Kingdom, lacked explicit use of an "equivalency" standard in their statutes, but called for treatment of transferred personal infor-

---

76 Explanatory Report to the Convention for the Protection of Individual with Regard to Automatic Processing of Personal Data ¶ 9, Jan. 28, 1981, E.T.S. No. 108.

77 *See, e.g.*, *id.* ("In order to counter this risk some countries have built into their domestic law special controls, for example in the form of a license for export.").

78 Convention 108, *supra* note 62, at art. 12(2).

79 *Id.* at art. 12(3)(a).

80 *Id.*

81 *See* Schwartz, *supra* note 23, at 478.

82 *See id.* at 473 ("Numerous European standards, national and supranational, permit the blockage of international flows of personal information.").

83 *Id.* at. 474–76.

84 *Id.* at 474.

mation in the receiving nation that would be consistent with native protection.[85] As for Germany, its federal data protection law offered a complex bifurcated scheme for public and private sector transfers.[86] At the time, however, scholars agreed that both statutory sections prohibited data transfers to nations whose protection was not equivalent to German standards.[87] Thus, before GATS, privacy law in the 1980s cast a shadow on international trade, which was the looming threat of data embargoes.

3. Present at the creation: the Uruguay Round.

When the Uruguay Round launched in Punta Del Este in 1986, in a process that would determine the new global international trading order, the relationship between privacy and trade was well established. Indeed, as demonstrated above, international guidelines as well as transnational instruments had developed a series of nascent responses to fears of imperiled global data flows.[88]

Moreover, the technology of the day, albeit quaint from today's perspective, had already increased international transmissions of information. At the time of the Uruguay Round, the tools for global data flows were largely mainframes and so-called minicomputers in the hands of governments and large private enterprises. To be sure, a decentralization of computing power had begun with the advent of the personal computer. In Switzerland in the 1980s, Tim Berners-Lee was working on the building blocks of the World Wide Web and was on his way to creating HTTP and HTML and developing the world's first web server.[89] In 1995, Bill Gates published *The Road Ahead* and boldly predicted that "[t]he information highway will transform our culture as dramatically as Gutenberg's press did the Middle Ages."[90] Gates pointed to how information and opportunity would soon spread across borders to developing nations due to "[c]heap global communications," which could "bring people anywhere into the mainstream of the world economy."[91]

---

85 *Id.* at 474–75.

86 Schwartz, *supra* note 23, at 475–77.

87 *Id.* at 476–77.

88 *See supra* Part I.A.2.

89 TIM BERNERS-LEE WITH MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB 35–51 (1999).

90 BILL GATES, THE ROAD AHEAD 9 (1995).

91 *Id.* at 261.

Throughout the 1980s, however, the rise of globally connected communication systems was based on proprietary computer networks. NSFNET, the precursor of today's Internet, was to be used for U.S. research and academic purposes alone.[92] The first commercial ISP, providing access to the internet to the general public, would not appear until November 1989.[93] In the private sector, the credit card industry was at the forefront of the burgeoning increase in global data flows. As an example, the *New York Times* reported in 1988 on Project Genesis at American Express, which was to allow this company "to standardize its data around the world—and develop powerful and comprehensive files on its cardholders."[94] One day, its benefits might even reach to allowing business travelers "to send and receive electronic mail at any American Express office and even plug into their own company's information systems."[95]

Against this background, there are surprising and unsurprising aspects of the focus during the Uruguay Round on avoiding local barriers to cross-border data flows. Today, several decades removed from these events, it is remarkable that international data flows were such a major concern of the negotiators. Yet, it is also predictable that the entities with the greatest interest in this subject proved to be large private organizations that were already investing in and benefiting from their own international data exchanges. As Dr. Juan Marchetti and Professor Petros Mavroidis explained in their history of GATS, American Express played a "pivotal" role in lobbying for the multilateral negotiations on trade in services.[96] Testifying in a 1984 House hearing on trade in services, Dr. Joan Spero, Executive Vice President of American Express, noted her company's reliance on cross-border data flows.

---

92 Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89, 110–12 (2001).

93 SIMSON L. GARFINKEL & RACHEL H. GRUNSPAN, THE COMPUTER BOOK: FROM THE ABACUS TO ARTIFICIAL INTELLIGENCE, 250 MILESTONES IN THE HISTORY OF COMPUTER SCIENCE 402 (2018).

94 John Markoff, *American Express Goes High-Tech*, N.Y. TIMES (July 31, 1988), https://www.nytimes.com/1988/07/31/business/american-express-goes-high-tech.html (noting that this project involved "120 mainframe computers, 170 minicomputers and 46,000 individual work stations").

95 *Id.*

96 Juan A. Marchetti & Petros C. Mavroidis, *The Genesis of the GATS (General Agreement on Trade in Services)*, 22 EUR. J. INT'L L. 689, 693 (2011). Even as early as the 1980s, American Express depended "on the rapid transmission of large amounts of data across national borders." *Id.* at 694.

Spero stated, "We simply could not function without rapid, unhindered global communications . . . . We use [them] to authorize a quarter million American Express card transactions each day throughout the world, with an average response time of 5 seconds."[97] American Express thus pressed the U.S. government for international rules that would defend the global flows essential to its business.

The debates within the Uruguay Round on the issue of privacy also confirm that certain EU states were key leaders—and the United States a laggard—when it came to including privacy protections in the international trade regime.[98] At the same time, however, the discussions show a remarkable ambivalence on how strongly to protect privacy, even on the part of European states. The Nordic countries were the first to propose that the trade negotiations respect privacy protections. Writing on behalf of the other Nordic countries in 1985, Sweden stated that "technological change will bring about increasingly rapid structural adjustment . . . . Trade in services, which is often intimately linked to high technology, will be highly affected by this development . . . . In many cases, it must be recognized that national regulations exist to safeguard legitimate precautionary interests (national security, personal privacy, etc.)."[99] It was fitting for Sweden to raise this concern; it had enacted the world's first national data protection law in May 1973.[100] At the same time, however, the Swedish

---

97 Service Industries: The Future Shape of the American Economy, Hearings Before the Subcomm. On Econ. Stabilization of the H. Comm. On Banking, Finance and Urban Affairs, 98th Cong. 369–70 (1984) (statement of Joan Edelman Spero, Senior Vice President, American Express Co.) [hereinafter 1984 Hearings].

98 *See, e.g.*, Yik-Chan Chin & Jingwu Zhao, *Governing Cross Border Data Flows: International Trade Agreements and Their Limits*, 63 LAWS 1, 5 (2022):

> As early as in the Uruguay Round of GATS negotiations . . . the EU insisted that the GATS agreement could not prevent member states from implementing and enforcing laws concerning "the protection of the privacy of individuals in relation to the processing and dissemination of personal data" . . . in order to prevent trade rules from affecting privacy protections.

Cf. Marchetti & Mavroidis, *supra* note 96, at 692–94 (noting the United States' focus on trade liberalization in the Uruguay Round).

99 Submission by the Nordic Countries (Finland, Iceland, Norway and Sweden) on Future Trade Negotiations in GATT 3, WTO Doc. L/5827 (July 5, 1985).

100 For background on Swedish data protection law, see DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 94–103 (1992).

submission to the trade negotiations warned of the need to "counteract protectionist and arbitrary elements in regulations concerning trade in services."[101]

A final lesson of a close study of the Uruguay Round debates is the forgotten role of developing countries in seeking explicit recognition of the inclusion of privacy in the international trade order. Developing countries are often viewed as lacking agency in the crafting of international institutions, but the negotiation history reveals a counternarrative. For example, India repeatedly pressed the importance of privacy protections in the Uruguay Round negotiations.[102] As early as 1986, India noted the "very specific considerations [with respect to services] such as . . . the need to preserve the cultural identity, sovereignty and national security, and the need to preserve the privacy of individuals."[103] Venezuela reserved concerns over privacy in its schedule of commitments under the GATS agreement. It explained that

> The Venezuelan Constitution protects personal privacy. It is therefore assumed that information will not be treated in any way contrary to this constitutional guarantee and that in any case the free consent of the persons to whom the information refers will be obtained prior to its provision, processing or transfer.[104]

During this same commitments phase, the Dominican Republic explained that its law recognized privacy as a basic worker right.[105]

Yet, privacy ultimately disappeared from the GATS agenda except for the Privacy Bracket. When the United States tabled its proposed text for the new agreement for trade in services in October 1989, privacy was nowhere to be found.[106] Then in June

---

101 Submission by the Nordic Countries, *supra* note 99, at 4. Later that year, Norway and Sweden proposed that the transmission of personal data across the border should be subject to privacy protection law. Note by the Secretariat, *Analytical Summary of Information Exchanged Among Contracting Parties*, *Revision*, ¶ 88, MDF/7/Rev.2 (Nov. 25, 1985).

102 GATT Services, *Draft Minutes of the Meeting Held on 17–18 April 1986*, ¶ 12, MDF/W-63 (May 5, 1986).

103 *Id.*

104 Communication From Venezuela, *Conditional Offer of Venezuela Concerning Initial Commitments in the Services Negotiations*, MTN.GNS/W/123/Add,1/Rev.2, at 20 (Apr. 9, 1992).

105 Communication From the Dominican Republic, *Conditional Offer of the Dominican Republican Concerning Initial Commitments on Trade in Services*, MTN.GNS/W/173, at 3 (Oct. 25, 1993).

106 Communication from the United States, *Agreement on Trade in Services*, art. 16, MTN.GNS/W/75 (Oct. 17, 1989). As if to emphasize its own priorities, the United States

1990, a proposal from the European Community, which was soon to become the European Union, included privacy among its exceptions, subject to significant conditions. Here were the basic elements of the Privacy Bracket: the parties may adopt or enforce measures "necessary to protect personal data and individual privacy" so long as "such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between parties where like conditions prevail, or a disguised restriction on international trade in services."[107] Japan's proposal the following month echoed this approach.[108] The final GATS text on the privacy exception tracked the 1990 proposals from the European Communities and Japan.[109]

Why was privacy simply bracketed in the international trade negotiations? There were clear global political economy concerns at play. The United States saw itself as a world leader in information services. In addition to American Express, other leading companies and industry organizations had testified in Congress in favor of extending trade disciplines into services. John Eger, the former Director of the Office of Telecommunications Policy, testifying in the House of Representatives in 1980, called the United States "the OPEC of information."[110] This comparison is telling: the U.S. economy had been crippled in 1973 and 1979 by OPEC's control over oil supply and prices.[111] By drawing an analogy with OPEC, Eger indicated that he anticipated a similar power for U.S. companies should the law permit them free access to information flows. Similarly, Spero of American Express labeled data flows "the lifeblood of virtually every major economic activity."[112]

---

did include exceptions for intellectual property and the prevention of fraud or deceptive practices; however, these exceptions did not make it into the final text. *Id.* at art. 16, ¶ 16.2.

107 Communication from the European Communities, *Proposal by the European Community, Draft, General Agreement on Trade in Services*, art. XV(1)(c), MTN.GNS/W/105 (June 18, 1990).

108 Communication from Japan, *Draft General Agreement on Trade in Services*, art. 607(2)(c), MTN.GNS/W/107 (July 10, 1990).

109 GATS, *supra* note 15, at art. XIV(c)(ii).

110 Frank Kuitenbrouwer, *The World Data War*, 91 NEW SCIENTIST 604, 604 (Sept. 3, 1981) (quoting John Eger).

111 Off. of the Historian, *Oil Embargo, 1973–1974*, U.S. DEP'T OF STATE, https://perma.cc/7ZNX-37YM; Samantha Gross, *What Iran's 1979 Revolution Meant for US and Global Oil Markets*, BROOKINGS INST. (Mar. 5, 2019), https://perma.cc/3AF8-7DYF.

112 1984 Hearings, *supra* note 97, at 380.

The United States' interests were clear, but what explains the Europeans agreeing to bracket privacy? By the conclusion of the Uruguay Round, the European Community had been replaced by the European Union, and, in an official statement at the time, it had announced, "The European Union accounts for 20% of world exports of goods and for *30% of exports of services*."[113] Given that the European Union was already more dependent on exporting services than goods, an international trade agreement, like GATS, that covered services would be a highly welcome development for it. European companies, like their U.S. counterparts, were global leaders in finance, insurance, and other professional services, and depended on cross-border data flows across the world.[114] As a consequence, like the United States, the European Union saw itself as a major beneficiary of free trade in services and the global data flows that they required.

Bracketing privacy allowed regulatory space for a country to provide privacy protections, but only if these safeguards did not unduly interfere with trade. With an eye to preserving international data transfers, both the United States and European Union viewed a strong GATS as helping to curb hurdles to such information flows. From their joint perspective, a GATS with a Privacy Bracket provided a short-term solution and a useful delaying tactic—it allowed a more complete resolution of a reconciliation of privacy and trade while also allowing countries to continue to develop data privacy law, but only when these laws were nondiscriminatory.

B. The Reckoning

The Bracketing left people across the world wondering whether their data could travel safely across borders. Each nation would have to decide for itself whether it was safe to send personal data to a foreign country. The Bracketing deferred to another day international decision-making about how privacy and trade were to be reconciled. To add to the complexity, each state could insist on its own rules, which ultimately varied widely across the world. Those rules would differ with respect to when and what data could be taken out of the country, what data could

---

113 *The Uruguay Round: Memo 94/24*, EUR. COMM'N (Apr. 12, 1994) (emphasis added), https://perma.cc/YY9V-VN9F.

114 Indeed, the European Union is now the world's largest exporter of services. *Trade in Goods and Services*, EUR. COMM'N, https://perma.cc/3LQJ-5XNR.

be collected, and how and why it could be processed and retained. While the Bracketing left each nation with the regulatory space to determine its own privacy laws, as long as they were not unduly trade restrictive, it also set the stage for today's crisis. Precisely when the internet made a truly global service possible even for small enterprises and individuals, a global service would become a huge challenge.

For much of the last quarter century, these worries proved largely theoretical. For one thing, many nations, including some in Europe, did not have data protection laws on the books until the last two decades.[115] But recent developments have brought us to crisis. To demonstrate the global privacy crisis resulting from the Bracketing, this Article proceeds as follows. First, based on a global review of data privacy laws, this Article shows that the fragmentation of the requirements for global data exchanges is even greater than many might imagine.[116] Second, this Article explores the regulatory thicket created by the numerous laws across the world.[117] Even a strategy of choosing the strictest law for an international enterprise will not work as a compliance strategy; as it turns out, no law is the strictest on all measures, not even the General Data Protection Regulation (GDPR) of the European Union.[118] Finally, this Part discusses the great burden that diverse data privacy laws place on smaller companies, including those in Europe.[119]

1. The splintering of adequacy.

Data privacy law has seen a remarkable diffusion of policy innovations among different countries. In this area, legal transplants are common. For example, California gave the world the first data-breach notification law, which many other jurisdictions have now adopted.[120] For international data flows, however, the

---

115 *See, e.g.*, Graham Greenleaf, *Countries with Data Privacy Laws — by Year 1973–2019*, 159 PRIV. L. & BUS. INT'L REP. 1, 1 (2019) [hereinafter Greenleaf, *Countries with Data Privacy Laws*].

116 *See infra* Part I.B.1.

117 *See infra* Part I.B.2.

118 *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 45, L 119/1 (May 5, 2016) [hereinafter GDPR].

119 *See infra* Part I.B.3.

120 Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 924 (2007).

contribution of the European Union has been decisive. The key EU idea is the necessity of a governmental power to block data flows to nations without "adequate" protection. This concept has now been adopted across the globe, but without any common substantive definition of adequacy or without any uniform process. The result has been a splintering of the "adequacy" principle. Each country defines it in different terms and applies it according to its own agenda.

This saga begins with the development of this concept in the European Union, which permits transfers of personal data to countries outside its borders (so-called "third countries") only if these nations have an "adequate" level of protection, as determined by the European Commission.[121] As for the substance of formal EU adequacy decisions, the Commission looks to a broad range of factors, now codified in the GDPR. It requires scrutiny of a variety of factors in a third country, such as the relevant legislation, the presence of rights for individuals, the safeguarding of judicial and administrative redress, and the availability of recourse to independent supervisory authorities.[122]

The constitutional underpinnings of data protection have also led to an important and continuing role for the Court of Justice of the European Union (CJEU) in scrutinizing the legality of adequacy determinations. In *Schrems v. Data Protection Commissioner* (*Schrems I*),[123] and again in *Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems* (*Schrems II*),[124] the CJEU determined that "adequacy" for data transfers meant a level that was "essentially equivalent" between the EU and the third country.[125] Case law of the CJEU, including both *Schrems* decisions, has also strengthened the role of independent data protection authorities in the member states.[126] In

---

121 For a discussion, see SOLOVE & SCHWARTZ, *supra* note 37, at 1265–67.

122 GDPR, *supra* note 118, at art. 45(2)(a).

123 *Schrems I*, *supra* note 2.

124 *Schrems II*, *supra* note 2.

125 *Schrems I*, *supra* note 2, at ¶¶ 73–74; *Schrems II*, *supra* note 2, at ¶¶ 198–202.

126 *Schrems II*, *supra* note 2, at ¶¶ 107–16; *Schrems I*, *supra* note 2, at ¶ 63; Case C-288/12, Eur. Comm'n v. Hungary, ECLI:EU:C:2014:237, ¶ 47 (Apr. 8, 2014); Case C-614/10, Eur. Comm'n v. Republic of Austria, ECLI:EU:C:2012:631, ¶ 66 (Oct. 16, 2012); Case C-518/07, Eur. Comm'n v. Germany, ECLI:EU:C:2010:125, ¶ 23 (Mar. 9, 2010). For a discussion of the need for these governmental officials to act with complete independence as anchored in the GDPR, see Thomas Zerdick, *Article 52 Independence*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 872, 875–82 (Christopher Kuner et al. eds., 2020).

Schrems II, for example, the Court found that each data protection authority is "vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down" in the GDPR.[127]

How then does the process of obtaining a formal "adequacy" determination from the European Union work? The applicable procedures are not for the faint of heart. Typically, the process begins with multiyear discussions and negotiations between the Commission and a third country.[128] These may require the country seeking the adequacy determination to amend its data privacy laws or to provide legally binding assurances to the European Union. The process then involves a proposal from the European Commission, an opinion of the European Data Protection Board, the approval of representatives of EU countries, and the adoption of a final decision by the European Commission.[129] At any time during this process, there is a possibility for involvement by the European Parliament and the Council of the European Union, which is a body of representatives of government ministers from each EU country.[130] The Parliament or Council can request that the Commission amend or withdraw an adequacy decision.[131]

As the rainbow that leads to a pot of gold, an adequacy determination places a third country on equal footing with any EU member state for purposes of cross-border data transfers. After the decision, the third country can receive personal data from the European Union without further requirements.[132] Yet, the resulting EU green list of adequate countries currently includes only eight nations outside of the European Union.[133] This result follows because, as noted in a leading German data protection treatise,

---

[127] *Schrems II*, *supra* note 2, at ¶ 107. For an introduction to the privacy and data protection jurisprudence of the CJEU, see ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 132–76 (2015).

[128] *Adequacy Decisions: How the EU Determines If a Non-EU Country Has an Adequate Level of Data Protection*, EUR. COMM'N [hereinafter EUR. COMM'N, *Adequacy Decisions*], https://perma.cc/RG7F-7ZDE.

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] The European Commission currently recognizes Argentina, Canada (commercial organizations), Israel, Japan, New Zealand, South Korea, the United Kingdom, and Uruguay as providing adequate protection. *See id.* Other adequacy rulings recognize European territories (Faroe Islands, Guernsey, Isle of Man, Jersey), a European principality with 77,000 people (Andorra), and Switzerland. *Id.*

the evaluation by the European Union of the level of data protection in a third country "is complex and prolonged."[134]

Contrast the scant number of nations on the European Union's approved list with the tally of the world's data privacy laws. Removing the twenty-seven EU member nations from the tally of 157 countries with such statutes leaves a stark result: the European Union has decided that significantly less than 10% of the world's data protection laws are adequate.[135] This low number is especially notable in light of the fact that most of the world's data privacy laws follow the European model.[136] The EU process for adequacy determinations appears incapable of keeping up with the rise of countries with statutes in this area and the increase in global data flows.

As a further complication, the European Union is not the only judge of the adequacy of privacy laws as many other nations have now taken on this role. While the European Union pioneered the adequacy approach, much of the world has embraced it. Our review of global data privacy laws reveals that there are now sixty-five countries outside the European Union whose data laws permit or require adequacy reviews of foreign jurisdictions before allowing international transfers of personal data from their borders.[137] Appendix A to this Article sets out these countries.

Why have so many countries adopted an adequacy approach? The Privacy Bracket seemed to leave the world with little other choice. The Bracketing left nations in search of mechanisms for safeguarding the personal information of their residents when it flowed across borders—as would increasingly occur in a world of trade in digital services and goods. At least in theory, a finding of adequacy offers the most trade-friendly solution to cross-border flows that is also consistent with ensuring a high level of privacy protection. If the foreign country's privacy protections are as good as one's own, then transferring the personal data internationally is like transferring it across the street. But highly idiosyncratic

---

134 Peter Schantz, *Artikel 45: Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses*, *in* DATENSCHUTZRECHT: DSGVO MIT BDSG [Data Protection Law: GDPR and the BDSG]) 970, 972 (Spiros Simitis et al. eds., 2019).

135 EUR. COMM'N, *Adequacy Decisions*, *supra* note 128; Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills*, 169 PRIV. L. & BUS. INT'L REP. 4–18 (2021).

136 Graham Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, 176 PRIV. L. & BUS. INT'L REP. 1, 8 (2022) [hereinafter Greenleaf, *Now 157 Countries*].

137 *See* Appendix A.

results have followed from both the result of the explosion in adequacy approaches and the activities of many governments now in the business of reviewing each other.

Russia, for example, declares all countries ratifying the Council of Europe's Convention 108 to be adequate—even without examining whether there is any domestic enforcement of the treaty provisions.[138] The Roskomnadzor, the Russian internet regulator, has also declared a number of countries adequate, including Argentina (which the European Union also declares adequate) but not Uruguay (unlike the European Union).[139] Also unlike the European Union, Russia has found adequate some countries in Africa, including Angola, Benin, Gabon, Mali, Morocco, South Africa, and Tunisia.[140] While the European Commission has repeatedly insisted on a highly specialized regime to protect data transferred to the United States,[141] Colombia, in contrast, has held the U.S. data protection law to be adequate without special provisions for the exchanged information.[142]

Moreover, the European Union's own use of adequacy proves problematic. As noted, the European Union has found only a handful of countries outside of Europe to be adequate. Moreover, in *Schrems I* and *Schrems II*, the CJEU invalidated data sharing agreements with the United States largely because of concerns about U.S. intelligence surveillance.[143] At the same time, however, EU member states have their own surveillance laws, as well as intelligence sharing arrangements with the United States, and it is not clear whether their own citizens have sufficient rights to challenge that surveillance.[144] The expansion of adequacy rules

---

[138] Maria Ostashenko, Irina Anyukhina & Anastasia Petrova, *Russia—Data Protection Overview*, ONETRUST DATAGUIDANCE (Apr. 2022), https://perma.cc/G7PX-FMGK.

[139] *Id.* Uruguay ratified Convention 108 in 2021. Newsroom, *Uruguay Ratifies Convention 108+*, COUNCIL OF EUR. (Aug. 9, 2021), https://perma.cc/935U-L6L9. Argentina also ratified Convention 108. Newsroom, *Argentina, 33rd Country to Sign Convention 108+*, COUNCIL OF EUR. (Sept. 19, 2019), https://perma.cc/G3WB-86JJ.

[140] *Russian Privacy Regulator Adds Countries to List of Nations with Sufficient Privacy Protections*, HUNTON ANDREWS KURTH (Aug. 16, 2017), https://perma.cc/E7NY-6PVX.

[141] Francesco Guarascio & Foo Yun Chee, *EU-U.S. Data Transfer Deal Cheers Business, but Worries Privacy Activists*, REUTERS (March 25, 2022), https://www.reuters.com/legal/litigation/eu-us-reach-preliminary-deal-avoid-disruption-data-flows-2022-03-25/.

[142] *Colombia Designates U.S. as "Adequate" Data Transfer Nation*, HUNTON ANDREWS KURTH (Aug. 15, 2017), https://perma.cc/DF29-ADEE; Guarascio & Chee, *supra* note 141.

[143] *Schrems I*, *supra* note 1, at ¶¶ 96–106; *Schrems II*, *supra* note 1, at ¶¶ 198–202.

[144] HENRY FARRELL & ABRAHAM NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 159 (2019); Paul Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, *in* BULK COLLECTION:

means that more countries will be inadequate to receive data without sometimes unwieldly legal safeguards in place. In sum, the explosion in adequacy standards may mean the implosion of trade.

2. The regulatory thicket.

The splintering of adequacy greatly complicates modern international trade, limiting the transfer of personal data across borders. But worldwide data flows face a further complication: The growing number of countries with comprehensive but varying data privacy law makes management of personal data a complex undertaking for any enterprise that hopes to operate across the globe. Even without any international transfers of data, the costs of compliance for a global entity are high because data privacy laws now create a dense thicket of rules that are nearly impossible to traverse.

According to a census of the world's data privacy laws, there are now 157 countries with such statutes.[145] Professor Graham Greenleaf, the census taker, has found that the number of countries enacting such legislation increased 10% from 2019 to 2020 alone.[146] Among the nations to join the data-privacy club during this period were Barbados, Botswana, Egypt, Jamaica, Nigeria, Togo, and Uzbekistan.[147] From 2020 to 2022, another twelve countries enacted data privacy laws, including Belize, Ecuador, Rwanda, Saudi Arabia, and Zambia.[148] This Article has already given one demonstration of the complexity of these laws in its discussion of adequacy.

As a further example of the complexity of global privacy laws, and one independent of cross-border data flows, we can examine legal regulation of the granting of consent to data processing. Consent is a linchpin issue: it is a core fair information practice, and one that has been long enshrined as providing a basis for the legal processing of personal data.[149] There are also now a dizzying range of parameters for acceptable consent in the world's data-

SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 61, 88–89 (Fred Cate & James X. Dempsey eds., 2017) (discussing cooperation between the NSA and the German Federal Intelligence Service).

145 *See generally* Greenleaf, *Now 157 Countries*, *supra* note 136.

146 Greenleaf, *Global Data Privacy Laws 2021*, *supra* note 1, at 1.

147 Greenleaf, *Data Privacy Laws 2021*, *supra* note 135, at 2.

148 *Id.* at 2–7.

149 *The Fair Information Principles*, PRIV. FIRST, https://perma.cc/S2EH-CY3E.

privacy statutes. This Section will look at five countries and one subjurisdiction, California, and explore different aspects of their regimes governing consent.[150] And here is a spoiler alert: there is no single organizational approach that will meet all global privacy rules for consent.

As a comparative matter, countries generally agree that consent with respect to data privacy requires that the "data subject"—that is, the affected party—be provided with sufficient information to make an informed decision. The surveyed jurisdictions also allow individuals to withdraw their consent subsequently. But the details concerning valid consent vary, and they do so widely.

Consider first the California Consumer Privacy Act[151] (CCPA), an influential state privacy law in the United States. As a promising initial step towards global uniformity, the CCPA borrows the language of the leading European data privacy law, the GDPR, requiring that consent be "freely given, specific, informed, and unambiguous."[152] So far so good, but the CCPA then permits an opt-out mechanism for obtaining consent for the sale of personal information.[153] An opt-out requirement means that organizations need not obtain users' agreement before processing of their personal data. Rather, an opt-out approach calls for permitting users to take affirmative action to indicate their refusal to personal data processing.[154] In contrast, the European Commission views consent under the GDPR as requiring a "positive act (for example an electronic tick-box that the individual has to explicitly check online or a signature on a form)."[155] This approach is quite different from California's opt-out approach to the sale of personal information.

---

150 These countries are Brazil, California, China, the European Union, India, and Japan. *See* Appendix B.

151 CAL. CIV. CODE § 1798.100 (2021) [hereinafter CCPA].

152 GDPR, *supra* note 118, at art. 4(11).

153 CCPA § 1798.120. Recent draft regulations from the California Privacy Protection Agency seek to police consumer consent, however, by taking steps to prevent businesses from manipulating individuals. *See, e.g.*, California Privacy Protection Agency, Title 11, Div. 6, Chap. 1, § 7025, Draft Regulations (June 2022), https://perma.cc/7ZNQ-JAJN (requiring opt-out preference signals that "provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing").

154 CCPA § 1798.135.

155 *When Is Consent Valid?*, EUR. COMM'N, https://perma.cc/9T8A-QD9T.

Japan, too, requires consent before the processing of personal information, subject to certain statutory exceptions.[156] At the same time, however, Japan permits an opt-out option for data transfers to a third party, but only when the transferor has obtained permission from the Personal Information Protection Commission of Japan for such transfers.[157] In contrast, the GDPR has no referral process permitting opt-out.

Often the relevant laws specify distinct requirements for certain situations. For example, Brazil calls for specific consent of the data subject in order for the controller (the data processing decisionmaker) to transfer personal data to another controller.[158] In the nomenclature of data privacy law, a data controller is the "person or organization . . . that determines the purposes of" an activity involving personal data.[159] In contrast, the GDPR does not have a special requirement for specific consent for data controller to data controller sharing. As one of the GDPR's special requirements, however, the European Data Protection Board (EDPB)—an independent European body composed of representatives of EU national data protection authorities—has interpreted it as forbidding the use of "pre-ticked boxes" to indicate agreement to data sharing.[160]

The survey of consent in these jurisdictions reveals differences even in something as seemingly straightforward as the age of consent for children. The issue is one of considerable practical importance. Below the statutory age, parents must consent before a company can collect personal information from the minor. At the age of consent and above, the individual can freely agree to collection and use of their information.

---

156 For an English translation, see Act on the Protection of Personal Information (Tentative translation), art. 16 (adopted May 23, 2003) (Japan) ("A personal information handling business operator shall not handle personal information without obtaining in advance a principal's consent.").

157 *Id.* at art. 23(2).

158 Lei Geral de Proteção de Dados Pessoais (LGPD), art. 7(X)(5) (adopted Aug. 14, 2018) (Braz.) [hereinafter LGPD].

159 AM. LAW INST., PRINCIPLES OF THE LAW, DATA PRIVACY Sec. 2(e) (2020); *see also* GDPR, *supra* note 118, at art 4(7).

160 EUR. DATA PROT. BD., GUIDELINES 05/2020 ON CONSENT UNDER REGULATION 2016/679, Version 1.1 ¶ 79 (adopted May 4, 2020). Under certain member state laws, such as those of Germany, consent to data processing for marketing purpose sometimes requires the use of not one, but two indications of consent ("double opt-in"). For a discussion, see MARTIN SCHIRMBACHER, ONLINE-MARKETING-UND SOCIAL-MEDIA-RECHT [Online Marketing and Social Media Law] 546–47 (2d ed. 2017).

Among the six jurisdictions surveyed, there are at least five different answers for what age a child must be before parental consent is no longer needed for collecting their information, as Appendix B to this Article shows. Brazil set the age at eighteen, Japan at fifteen, China at fourteen, and California at thirteen.[161] The European Union sets the age of consent at sixteen, but with an "opening clause" permitting member states to lower it to thirteen, and different member states have adopted every age possible between thirteen and sixteen.[162]

This Article's multijurisdictional inquiry shows how tricky it is to obtain consent from data subjects, whether from children or from adults. This task cannot be resolved by simply adopting the strictest rule because no law is strictest on all measures. Recourse is simply not possible to the GDPR because there is no uniform age set for children's age in the Union. Nine members of the European Union have selected thirteen years as the age of consent, six have chosen fourteen years, three have opted for fifteen years, and ten have remained with the GDPR's default of sixteen years.[163] Satisfying the consent requirement of any of these jurisdictions does not necessarily satisfy the consent requirement of all of the others.

Finally, many laws go beyond the GDPR's requirements in additional ways. For example, the GDPR calls for clarity and intelligibility in its access and notice rights, but the CCPA requires

---

161 *See* Ana Carolina Cagnoni, *How Brazil Regulates Children's Privacy and What to Expect Under the New Data Protection Law*, IAPP (Oct. 29, 2019), https://perma.cc/7FMT-FSBU; *Global Data Privacy and Security Handbook: Japan*, BAKER MCKENZIE, https://perma.cc/BV9B-3YV6; STATE ADMIN. FOR MKT. SUPERVISION OF THE PEOPLE'S REPUBLIC OF CHINA, INFORMATION SECURITY TECHNOLOGY—PERSONAL INFORMATION (PI) SECURITY SPECIFICATION (effective Oct. 01, 2020), Mar. 6, 2020, at sec. 5.4(d), https://perma.cc/M7ZW-C3X2 ("[B]efore the collection of personal information of minors at 14 years old and above, the PI Controllers shall obtain explicit consent from the minors or their guardians; for minors under 14 years old, explicit consent from their guardians is required."); CCPA § 1798.120(c). India has proposed changing the age of consent to eighteen, but it has not yet done so. *See* Sameer Yasir & Karan Deep Singh, *India Withdraws a Proposed Law on Data Protection*, N.Y. TIMES (Aug. 4, 2022), https://perma.cc/EN4V-MNH4. For children between thirteen and sixteen, California requires an opt-in approach for the sale of their personal information (unlike the opt-out approach available for anyone sixteen years or older). CCPA § 1798.120(c).

162 GDPR, *supra* note 118, at art. 8.(1); Claire Quinn, *GDPR Age of "Digital" Consent*, PRIVO, https://perma.cc/2SQ2-YZUZ. This provision is a so-called "opening clause" in the GDPR, permitting national variation from a default. Emilia Mišćenić & Anna-Lena Hoffmann, *The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)*, 4 EU & COMPAR. L. ISSUES & CHALLENGES SERIES 44, 51–55 (2020).

163 Quinn, *supra* note 162.

companies to provide a toll-free telephone number or email address for consumers to make access requests.[164] The CCPA is also generally more prescriptive about the mode and content of notice at collection.[165]

3. Harm to small and medium enterprises, but a boon to large companies.

What are the problems caused by the failure to resolve the conflict between privacy and trade? The end result of the current situation is that only the largest companies and organizations can manage the globalization of data trade. At one time, the internet seemed to promise empowerment for all, including small companies in the world's poorest countries, which were expected to reach the world's richest markets.[166] The hope was for a democratization of trade and a resulting chance for a new global distribution of economic opportunities. But, increasingly, the reality is that only the world's richest companies can manage internet globalization.

The consequence of the regulatory thicket and splintering of adequacy has been harm to small and medium enterprises (SMEs), especially in less developed countries, and a boon to large companies, especially those in the West. Since many of the established tech companies are based in the United States, this result may further favor that side of the Atlantic.[167] This possibility is surprising and counterintuitive, especially in light of the sometimes-expressed opinion that European data protection law will tilt the playing field in favor of EU companies.[168]

Thus far, this Article has demonstrated the increasing complexity of global data privacy law. In response, data privacy law

---

164 CCPA § 1798.130.

165 Final Text of Proposed Regulations, California Consumer Privacy Act Regulations, § 999.305 (2020). California even encourages the use of a particular icon to opt-out of the sale of one's information, along with specific alt-text for visually impaired persons. Rob Bonta, Cal. Att'y Gen., *CCPA Opt-Out Icon*, CAL. DEP'T JUST., OFF. OF THE ATT'Y GEN., https://perma.cc/JCY4-TXFD.

166 ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD IN COMMERCE 12, 18–19 (2013).

167 Leonid Bershidsky, *Europe's Privacy Rules are Having Unintended Consequences*, BLOOMBERG (Nov. 14, 2018), https://perma.cc/7FZK-BVB2.

168 In the words of President Barack Obama in 2015, "[O]ften times what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests." Henry Farrell, *Obama Says That Europeans Are Using Privacy Rules to Protect Their Firms Against U.S. Competition. Is He Right?*, WASH. POST. (Feb. 17, 2015), https://perma.cc/RH7E-JWW5.

has undergone a shift to a compliance-focus and a heavy "managerialization."[169] Professor Ari Waldman has mapped how data privacy law promotes the creation of a new class of privacy compliance professionals who "create internal structures to comply with their version of the law."[170] Building on Waldman, we wish to suggest that this "managerialization" of privacy compliance inherently favors large companies and also has consequences for global distributive justice. Indeed, and as noted above, the result may favor technology companies in the United States. Many of the largest tech enterprises are in the United States, and these are the organizations that have invested heavily in the process of privacy compliance.[171]

There is more involved, however, than the legal savvy and financial resources available to these companies. U.S.-based tech companies begin with a significant global advantage due to their extensive customer base. By having this existing relationship with millions or even billions of customers throughout the world, it is easier for these enterprises to craft processes to comply with changing legal requirements while also maintaining data-rich relationships with their current users.[172] These connections provide a major head start on any startup. Thus, Apple's changes to its operating system in June 2021 that were announced as promoting privacy also serve to entrench its favorable market position by leveraging its own digital ecosystem.[173]

Similar conclusions have been reached regarding the competitive effects of the GDPR. Professor Michal Gal and data privacy specialist Oshrit Aviv argue that this law, "the Magna Carta" of data protection, "may limit competition and increase market concentration."[174] The GDPR does so by harming the ability of "small

---

169 Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 26 (2021).

170 ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 130 (2021).

171 *See, e.g.*, Ashley Rodriguez, *Google Says It Spent "Hundreds of Years of Human Time" Complying with Europe's Privacy Rules*, QUARTZ (Sept. 26, 2018), https://perma.cc/P4CX-WSFF.

172 Nick Kostov & Sam Schechner, *GDPR Has Been a Boon for Google and Facebook*, WALL ST. J. (June 17, 2019), https://perma.cc/Y68C-8JW9 ("[Tech giants] have direct relationships with consumers that use their products, allowing them to ask for consent directly from a much larger pool of individuals."); Jedidiah Yueh, *GDPR Will Make Big Tech Even Bigger*, FORBES (June 26, 2018), https://perma.cc/6UXR-CR9Z.

173 Kif Leswing, *Apple Is Turning Privacy into a Business Advantage, Not Just a Marketing Slogan*, CNBC (June 7, 2021), https://perma.cc/7MAN-2MVX.

174 Michal S. Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 16 J. COMPETITION L. & ECON. 349, 353, 386 (2020) ("The GDPR might also generate advantages for larger firms, thereby reducing potential competition.").

entrants" to collect personal data; limiting the economic incentives for sharing such data once collected; favoring internal collection of data; and creating uncertainty, which imposes higher costs on smaller players.[175] The economies of scale for compliance with privacy regulations favor larger firms. In their view, "the larger the firm, the lower its per-datum compliance costs, relative to smaller firms which must also comply with similar requirements."[176]

A window into this unintended tilting in favor of larger companies was provided in the aftermath of *Schrems II*, the decision of the CJEU in 2020 that invalidated the Privacy Shield, a data-transfer agreement between the European Union and the United States.[177] Following this judgment, the EDPB offered proposed guidance on cross-border data flows.[178] The hundreds of comments offered to the EDPB in response paint a revealing picture of the myriad ways that hurdles to cross-border data flows harm smaller companies and even *European* enterprises.

The responses to the EDPB begin by touching on issues such as intercompany data transfers for human resource data in an international enterprise, the possible isolation of Europe from the global economy, and even the loss of essential technological services offered by U.S. companies.[179] Perhaps surprisingly, however, startup associations across the European Union also criticized the proposed rules as harmful to their growth. For example, app developers in Belgium worried that the EDPB guidelines would disadvantage small businesses, which, according to them, made up "70 percent of the participants of the Privacy Shield."[180] Another

---

[175] *Id.* at 370–76.

[176] *Id.* at 370.

[177] SOLOVE & SCHWARTZ, *supra* note 37, at 1283–95; Anupam Chander, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771, 774 (2020); Nigel Cory, Daniel Castro & Ellysse Dick, *"*Schrems II*": What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, INFO. TECH. & INNOVATION FOUND. (Dec. 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/.

[178] *See generally Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protections of Personal Data*, EUR. DATA PROT. BD. (Nov. 10, 2020), https://perma.cc/38WC-EXUY.

[179] German Individual, *Comment R01/2020-0005* (Nov. 19, 2020), https://perma.cc/7SY9-PNBU; Employers of Poland, Comment R01/2020-0011 (Nov. 30, 2020), https://perma.cc/88KU-YZQT; Asesores Jurídicos Alemany y Asociados, *Comment R01/2020-0004* (Nov. 17, 2020), https://perma.cc/C7YK-22D7.

[180] ACT | The App Association, *Comment R01/2020-0013* (Nov. 30, 2020), https://perma.cc/RQ6H-VT7M.

Belgium-based group, Allied for Startups, worried about the "additional costs" of the supplementary measures that the EDPB would require for cross-border transfers, noting that "startups have less resources, less time and oftentimes operate with new technologies."[181]

The theme of excessive costs was sounded time and time again in the submissions to the EDPB. Danish entrepreneurs argued that the EDPB's supplemental measures "fail to acknowledge the reality of startups," which "will simply not be able to afford" to conduct "a detailed analysis of the characteristics of every transfer and an assessment of all applicable local laws requiring specialist multi-jurisdictional legal advice."[182] Their trade organization continued, "In practice, this would prohibit start-ups and scale-ups from relying on many global service providers . . . ."[183] A Spanish digital industry association worried that the rules "will require EU organisations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for most small and medium-sized enterprises, research institutions, and others."[184]

The EDPB responded to the comments by slightly modifying its rules.[185] These modifications generally do not lessen the harms that the companies feared. Indeed, the greatest concession of the EU regulators was to make it clear that the exporter could consider in its risk assessment "the practical experience of the importer, among other elements and with certain caveats."[186] The risk assessment itself requires the exporter to consider "the laws and the practices applicable to the importer and the data transferred," including no fewer than eleven possible sources—including case law of the CJEU and the European Court of Human

---

[181] Allied for Startups, *Comment R01/2020-0028* (Dec. 14, 2020), https://perma.cc/H5XF-V7ZP.

[182] Danish Entrepreneurs, *Comment R01/2020-0030* (Dec. 16, 2020), https://perma.cc/W8QG-8TQH.

[183] *Id.*

[184] AMETIC, *Comment R01/2020-0012* (Nov. 30, 2020), https://perma.cc/LF88-G3ZY.

[185] For an explanation of the changes, see *Privacy Matters: EDPB Adopts Final Recommendations on Supplementary Measures*, DLA PIPER (June 23, 2021), https://perma.cc/X4L8-3C9F.

[186] *EDPB Adopts Final Version of Recommendations on Supplementary Measures, Letter to EU Institutions on the Privacy and Data Protection Aspects of a Possible Digital Euro, and Designates Three EDPB Members to the ETIAS Fundamental Rights Guidance Board*, EUR. DATA PROT. BD. (June 21, 2021), https://perma.cc/4KDX-BUYR.

Rights, adequacy decisions in the country of destination, resolution and reports from intergovernmental organizations, national caselaw or decisions taken by administrative authorities, and "[r]eports based on practical experience with prior instances of requests for disclosure from public authorities."[187] It is difficult to imagine how any entity other than the largest resource-rich organizations will be able to comply with these requirements.

II. BEYOND THE BRACKET: EMERGING APPROACHES

The decision at the dawn of the internet age to bracket privacy in the modern trade order set the stage for the privacy-or-trade crisis that we face today. Part I of this Article demonstrated that while cross-border data flows are widely acknowledged as essential to contemporary trade, data privacy law has led to a splintering of the important adequacy norm for transfers, a regulatory thicket, and harm to SMEs and the developing world.

This Part turns to the emerging responses to this crisis and identifies three major approaches to the privacy-trade conflict. Professor Jagdish Bhagwati, one of the world's most distinguished trade economists, has described the emergence of bilateral and regional free trade agreements as creating a "spaghetti bowl" of "criss-crossing" trade rules with complicated rules of origin and complex sets of obligations.[188] This metaphor seems apt as well for the emerging data trade order. There are now different types of pasta in the spaghetti bowl of contemporary trade agreements. A nation typically does not adopt a single solution to the question of "privacy and/or trade," but accepts a range of different approaches as reflected in its own criss-crossing obligations.

This Part begins with the U.S. model, which favors trade over privacy,[189] and then turns to the European model,[190] which prioritizes privacy over trade. This Part then shows the emergence of a third model, a kind of escape valve, upon which both the United States and the European Union have converged.[191] In the United

---

[187] *Recommendations Version 2.0, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protections of Personal Data*, ¶ 144 EUR. DATA PROT. BD. (adopted June 18, 2021) [hereinafter *Recommendations Version 2.0*], https://perma.cc/TQ5L-NAQP.

[188] JAGDISH BHAGWATI, FREE TRADE TODAY 112–13 (2002).

[189] *See infra* Part II.A.

[190] *See infra* Part II.B.

[191] *See infra* Part II.C.

States and the European Union, accountability mechanisms permit private sector organizations to accept certain established data-privacy standards. The result is to release pressure that each system's predominant regulatory approach creates within international economic relations. These opt-in mechanisms allow recourse to second-best solutions that distribute decision-making power among a diverse set of institutions.

A. Trade Before Privacy

Given a choice, the United States would have the world regulate data privacy through national law and create bilateral and regional agreements that favor data flow. It has expressed this policy preference in various agreements, such as the United States–Mexico–Canada Agreement (USMCA).

1. The model in a nutshell.

The approach of the United States to data trade consists of three essential elements. First, it prioritizes the free flow of data across borders and does so by seeking binding trade rules promoting cross-border data flows. Second, the United States generally prefers national rather than international approaches to data privacy. In effect, the United States seeks globalized rules for trade but national rules for privacy. Third, the United States requires that privacy rules in other countries that interfere with the free flow of data across borders be strictly justified. This dynamic inevitably creates conflict among nations, for which the United States makes use of opt-in agreements to meet the demands of national privacy law.

2. Elements of the U.S. model.

As we have seen, since the 1980s, the United States, worried that national restrictions on data would imperil its multinational corporations, has sought to ensure the cross-border flow of data. Accordingly, it subjects such national data rules to international trade law disciplines. Here is the first element of its model: the United States seeks international trade agreements that protect cross-border data flows.

This story begins with the United States' role in shaping GATS. The United States was willing to have GATS recognize the importance of privacy, but it also wished it to limit privacy

measures to keep the WTO from unduly restricting trade.[192] The result was a stopgap—namely, the compromise that this Article terms the "Privacy Bracket." Left to its own devices, however, the United States sought to establish the primacy of trade over privacy in a series of bilateral and regional trade agreements. The United States set in place explicit protections for cross-border data flows in its trade agreements. These began with a requirement to "refrain from . . . unnecessary barriers to electronic information flows across borders" in the U.S.-Korea Free Trade Agreement.[193] As a further example, before withdrawing from the Trans-Pacific Partnership, the United States negotiated a robust set of rules favoring data flows, which were adopted by the remaining parties as part of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).[194]

Second, the United States does not seek to globalize privacy standards but to encourage national solutions. As the United States is the great international outlier in its legal system for data privacy, a globalization of norms in this area would likely work to heighten Europe's influence and favor its own framework. Where most of the rest of the world has enacted overarching data protection statutes, bolstered in places by narrower sectoral laws, the United States remains committed to its sectoral, patchwork approach—at least at the federal level.[195] In addition, the establishment of independent national data protection commissioners, a cornerstone of the approach in the European Union, is now common from Austria to Zambia.[196] The United States lacks any such national authority.[197] For example, the CPTPP introduces a requirement that each party maintain a legal framework for the protection of personal information, but it adds a footnote, one

---

192 *See supra* Part I.A.3.

193 Free Trade Agreement Between the Republic of Korea and the United States of America, art. 15.8, June 30, 2007, *modified*, Dec. 5, 2010.

194 Comprehensive and Progressive Agreement for Trans-Pacific Partnership, arts. 14.11, 14.13, Mar. 8, 2018 [hereinafter CPTPP]. The other eleven negotiating states adopted the free flow provisions in the final text of the CPTPP, which was the first treaty "to explicitly restrict the use of data localization measures." Burri, *supra* note 55, at 71.

195 *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy*, 105 MINN. L. REV. 1733, 1748 (2021).

196 *See* Republik Österreich: Datenschutzbehörde, EUR. L. INST., https://perma.cc/C6WP-VP35; *see also* Nat'l Assembly of Zambia, *Report of the Committee on Media, Information and Communication Technologies on the Data Protection Bill, N.A.B. No. 28 of 2020, Fifth Session of the Twelfth National Assembly*, § 7 (2021), https://perma.cc/AC2Q-FKYY.

197 For a call made two decades ago for a federal privacy agency in the United States, see Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1188 (2003).

clearly drafted by U.S. negotiators, that explains that a country can satisfy that requirement through "sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy."[198]

Third, the United States has sought to ensure that privacy measures that would limit the flow of personal data be strictly justified. To be sure, this requirement is, at least in theory, found in GATS. Article XIV(c)(ii) of that treaty requires trade-restrictive measures, such as ones protecting privacy, to be "necessary."[199] This language is much ignored, however, and the United States has, in turn, sought to make free flows of data more of an affirmative obligation in negotiating regional trade agreements.

With the USMCA in 2020, the United States found a way to do so. Here, the United States implemented the strongest currently existing version of a free-flow commitment. This free trade agreement is the first in the world to contain a "digital trade" chapter. Under it, no party can restrict the transfer of personal information across borders, unless such a restriction is necessary for a legitimate public purpose, not applied in a discriminatory manner, and not more restrictive than necessary for that purpose.[200] As Yakovleva pointed out, the USMCA is building in obligations that normalize privacy measures "as tools of international trade" and that views them as "trade values" rather than human rights.[201] A deeper look at the USMCA is merited at this juncture because this type of agreement represents the future if the United States gets its way.

The USMCA achieves its goals first by making it clear that it considers information privacy as a category of consumer protection law. Fittingly for this vision, it places its provisions about "Personal Information Protection" immediately after those for "Online Consumer Protection."[202] It begins its privacy section by stating that the parties to the agreement "recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing

---

198 CPTPP, *supra* note 194, at art. 14.8, n.6.

199 GATS, *supra* note 15, at art. XIV(c)(ii).

200 United States–Mexico–Canada Agreement art. 19:11, Nov. 30, 2018, 134 Stat. 11 [hereinafter USMCA].

201 Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416, 492 (2020).

202 USMCA, *supra* note 200, at arts. 19.7–19.8.

consumer confidence in digital trade."[203] This language is true to the U.S. paradigm that information privacy law serves to safeguard the individual as a consumer in the data marketplace.[204]

The USMCA's next step is to require the establishment of a legal framework for the protection of the personal information. It sets out certain key principles that the required data-privacy framework must contain. In particular, the USMCA references the APEC Privacy Framework and the OECD Guidelines on Privacy. Yakovleva rightly observes that these two international documents embody "the economic approach to the protection of personal data as a precondition for digital trade."[205]

The USMCA also makes clear that each country may devise its own data privacy rules. There are to be many rooms in the global house of privacy. The goal is not the uniformity of data privacy law, but interoperability of different regimes. As the USMCA states, "Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes."[206] This language is reminiscent of a project of U.S. corporate interests in the early part of the twenty-first century to reorient international privacy law around concepts of "interoperability" and "accountability."[207] The Global Accountability Project's 2009 Galway Paper, for example, sought to shift governance to individual organizations and to make it "a mechanism for global governance of data."[208] And "interoperability" was a key goal of the Obama Administration. Its 2012 report on "Consumer Data Privacy in a Networked World" called for engagement among "international partners to create

---

[203] *Id.* at art. 19.8(1).

[204] Schwartz & Peifer, *supra* note 35, at 147–49.

[205] Yakovleva, *supra* note 201, at 492.

[206] USMCA, *supra* note 200, at art. 19.8(6).

[207] Privacy and Information Security Law Blog, *Centre Testifies at ITC Hearing on Privacy as a Trade Barrier*, HUNTON ANDREWS KURTH (Mar. 7, 2013), https://perma.cc/D4AB-WJR7.

[208] CTR. FOR INFO. POL'Y LEADERSHIP, DATA PROTECTION ACCOUNTABILITY: THE ESSENTIAL ELEMENTS 1 (2009).

greater interoperability among our respective privacy frameworks."[209] This report begins with the observation that "governments may take different approaches" to "[c]onsumer data privacy frameworks."[210]

Looking to the future, we think that the United States will seek to expand the influence for its policy emphasis of trade before privacy. It is likely to develop new global trade arrangements to further the international flow of data. As in the USMCA, the United States will seek digital trade arrangements that consider privacy in consumer protection terms and allow considerable leeway to countries to find their own path.

The difficulty with different approaches, however, is that one nation may find a foreign nation's privacy framework to be lacking or "inadequate." If each country devises its own data privacy rules, it is understandable that countries will seek mechanisms to protect personal data as it flows abroad. The United States seeks to resolve possible tensions among these myriad approaches by allowing recourse to opt-in accountability mechanisms at the organizational level—as we discuss in the third model below. For example, the USMCA commits to recognize the APEC Cross-Border Privacy Rules (CBPR) as a sufficient safeguard for the cross-border flow of personal information.[211] Before exploring this system, this Article first turns to the European Union's model for global data exchanges.

B. Privacy Before Trade

The European Union would have the world favor data privacy over trade. But in various trade agreements and policy instruments, it has also sought to advance global data flows and, as a practical matter, has increasingly engaged in a coordination of privacy and trade negotiations.

1. The model in a nutshell.

The European Union's approach to international exchanges of personal data consists of three essential elements. First, in the European Union, privacy represents a higher value than trade in

---

[209] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY i–ii (2012).

[210] *Id.* at 31.

[211] USMCA, *supra* note 200, at art. 19.8(6).

data. Foundational documents of the European Union safeguard data protection as a fundamental right, and the CJEU vigorously enforces it. Second, at the same time as the European Union views privacy as a human right, it has sought to promote the free flow of personal data. It has developed the idea of "adequacy" as the essential substantive concept for deciding when personal information may leave the territory of the European Economic Area. But, as in the United States, the European Union permits the use of opt-in accountability mechanisms as an escape valve. Third, the European Union continues to maintain the ideology of the Bracket but, in practice, is coordinating its privacy and trade negotiations and doing so to heighten its influence.

2. Elements of the EU model.

The first element of the European Union's model for cross-border exchanges of personal data is its bedrock concept that privacy is a human right. Global transfers cannot undermine this interest. As the GDPR declares in its first recital, "The protection of natural persons in relation to the processing of personal data is a fundamental right."[212] A later recital confirms the desire to "further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations," but only "while ensuring a high level of the protection of personal data."[213] The constitutional status of data protection and privacy in the European Union is made explicit in two of its foundational documents, the Charter of Fundamental Rights and the Treaty on the Functioning of the European Union.[214]

While the European Union emphasizes the fundamental nature of the right to privacy, it has also sought to promote the global exchange of personal information. Thus, the second element of the EU model for data trade begins with a firm recognition of the economic value of information, which then leads to its

---

212 GDPR, *supra* note 118, at Recital 1.

213 *Id.* at Recital 6. A later recital in the GDPR, Recital 101, explicitly references the value of transnational exchanges of personal data. It states, "Flows of personal data to and from countries outside the Union . . . are necessary for the expansion of international trade and international cooperation." *Id.* at Recital 101. Yet, these transfers should not be at the cost of "the level" of data protection "ensured in the Union." *Id.*

214 Charter of Fundamental Rights of the European Union art. 8(1), 2000 O.J. (C 364/01) [hereinafter Charter] ("Everyone has the right to the protection of personal data concerning him or her."); Consolidated Version of the Treaty on the Functioning of the European Union art. 16(1), 2010 O.J. (C 83/47) ("Everyone has the right to the protection of personal data concerning them.").

"adequacy" approach. The European Union seeks to combine economic liberalization of personal data trade with harmonized policies to protect data privacy. A key early document in this regard was the Data Protection Directive (1995), which articulates its goals as (1) facilitating the free flow of personal data within the European Union and (2) ensuring an equally high level of protection within all EU countries for "the fundamental rights and freedoms of natural persons, and in particular their right to privacy."[215] The goal, one further developed through enactment of the GDPR, is to promote the free flow of personal data within the territory of the European Union by requiring a similarly high standard of data protection for all EU member states.[216] Hence, should personal information be transferred from France to Italy to Germany to Portugal, the data would be subject to the same rigorous rules.

As regards transfers outside of its borders, the European Union has long sought protection that follows personal data. Globalization of data flows required an international reach for EU data protection law. As Professor Spiros Simitis, an academic celebrated as a founder of European privacy law, stated, "Data protection does not stop at national borders."[217] And this policy imperative brings us to the adequacy idea. This Article has already described the widespread international adoption of the European Union's idea of adequacy, the process for achieving a formal adequacy decision from the Union, and the international splintering of this concept with sixty-five countries outside of the European Union adopting their own adequacy regimes. For the European Union, however, adequacy became a core principle for permitting trade in personal data as part of its protection of data privacy. Having achieved harmonized data protection within the territory of the European Union, it sought to prevent personal information from flowing to countries outside its borders with insufficient protection. The answer was to require these so-called "third countries" to have (at least) adequate protection.

Once adequacy was developed as the key EU standard, a policy debate ensued regarding whether this term indicated that

---

215 Directive 95/46/EC of the European Parliament and of the Council art. 1, 1995 O.J. (L 281) ¶ 1.

216 *Id.* at Preamble ¶ 3, arts. 1 & 25.

217 Spiros Simitis, *Einleitung: Geschichte — Ziele — Prinzipien* [Introduction: History — Goals — Principles], *in* KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [Commentary on the Federal Data Protection Law] 125 (Spiros Simitis ed., 7th ed. 2011).

non-EU countries might be permitted to have a lesser level of data privacy and still be eligible to receive personal data from EU member states.[218] And, as noted earlier in this Article, the CJEU decisively answered this question on two occasions. In its path-breaking decisions in *Schrems I* and *Schrems II*, it ruled that adequacy required no less than "essentially equivalent" levels of data protection between the European Union and a third country.[219] Thus, the EU model contains policy elements that favor privacy over trade. Data privacy has a normative backstop of an explicit constitutional status in the European Union and an institutional backstop in the form of a high court (the CJEU) eager to promote and enhance it.

There is also an escape valve for the EU model and its orientation around trade before privacy. In particular, the European Union has long been skeptical of the far different approach to data privacy in the United States.[220] These include matters such as the lack of an overarching statute and the absence of a human rights status for the privacy of personal information. The solution has been to negotiate opt-in standards for U.S. companies that wish to receive data transfers for Europe. We discuss these accountability mechanisms in the following section.

The third and final element in the EU model is an increasing coordination of trade and privacy efforts. Officially, the European Union claims to keep a wall between its trade policies and privacy protection. As the Commission stated in 2017, "[T]he protection of personal data is non-negotiable in trade agreements."[221] Following its adequacy decision for Japan, the Commission loftily observed, "For the EU privacy is not a commodity to be traded. Dialogues on data protection and trade negotiations with third countries have to follow separate tracks."[222] In practice, the European Union has launched adequacy negotiations simultaneously with trade negotiations. The EU-Japan adequacy agreement was negotiated in tandem with negotiations for the

---

[218] *Id.*

[219] *Schrems I*, *supra* note 2, at ¶¶ 73–74, 96; *Schrems II*, *supra* note 2, at ¶¶ 96, 104.

[220] *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1968, 1974, 1984 (2013).

[221] European Parliament Resolution of 12 December 2017 on "Towards a Digital Trade Strategy" (2017/2065(INI)), 2018 O.J. (C 369/03) ¶ V.

[222] Press Release, *Digital Single Market—Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers (MEMO/17/15)*, EUR. COMM'N (Jan. 10, 2017) [hereinafter *Digital Single Market*], https://perma.cc/5FP6-3ZF3.

EU-Japan Economic Partnership Agreement.[223] The Commission adopted the adequacy decision on January 23, 2019, and the Economic Partnership Agreement on February 1, 2019, in a one-two demonstration of syncing up the two matters.[224]

Crucially, the data trade negotiations between the European Union and Japan have now led to the world's first mutual adequacy agreement. Both countries recognize each other as providing an equivalent level of protection for personal data. Announcing the mutual adequacy decisions, the Commission heralded "the world's largest area of safe data flows." It made extensive references to the economic benefits that would flow accordingly, including "privileged access [for European companies] to the 127 million Japanese consumers."[225]

The coordination of these negotiations around trade and privacy, while maintaining formal separation, also illustrates a larger point, which is that adequacy findings have always contained a political element. Already in 2013, Kuner noted the difficulty of passing judgment "on a foreign regulatory system without political considerations playing some role."[226] Indeed, the Commission itself has acknowledged the instrumental nature of its process for selecting third countries for "a dialogue" on adequacy. In a 2017 white paper setting out its goals in this regard, the Commission's first consideration focused on trade: namely, "the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations."[227] The Commission's white paper also points to "the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at [the] international level."[228] A final factor makes clear the European Union's goal of

---

[223] *See generally* Paula Cisneros Cristóbal, *The Economic Partnership Agreement Between Japan and the European Union: Analysis of the First Years of Life and Prospects for the Future*, 13 AUSTL. AND N.Z. J. OF EUR. STUD. 55 (2021).

[224] Press Release, *European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (IP/19/421)*, EUR. COMM'N (Jan. 23, 2019) [hereinafter *European Commission Adopts Adequacy Decision on Japan*], https://perma.cc/GTH8-CFBD; Press Release, *EU-Japan Trade Agreement Enters into Force (IP/19/785)*, EUR. COMM'N (Jan. 31, 2019), https://perma.cc/SMK3-73F4.

[225] Press Release, *The European Union and Japan Agreed to Create the World's Largest Area of Safe Data Flows (IP/18/4501)*, EUR. COMM'N (July 17, 2018) [hereinafter *The European Union and Japan Agreed*], https://perma.cc/4EDW-ZAZ5.

[226] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 66 (2013).

[227] *Digital Single Market*, *supra* note 222, at 2.

[228] *Id.*

promoting widespread adoption of its policy balance: it will consider "the pioneering role the third country plays in the field of privacy and data protection" and whether this country "could serve as a model for other countries in its region."[229] Thus, in opening adequacy discussions, the European Union seeks to expand both its commercial relations with other countries and the influence of its regime for privacy protection.

Looking into our crystal ball, we think that the future path of the EU model will be continuing attempts by it to leverage its adequacy mechanism. Some nations will follow the recent path of Japan and South Korea by seeking a formal finding of adequacy from the Union. These countries will modify their laws and, like Japan, perhaps offer special protections for data originating in the European Union.[230] Thus, there will be the emergence of an "internal splintering" of data protection regimes with different standards *within the same country* depending on whether data originate in the European Union or domestically.

The Commission will also continue on the path of greater rigor and more demands in terms of required changes to national laws. The risk is that such incrementalism will place formal adequacy findings out of reach for developing nations. Overall, the result will be heightened compliance costs, which will create larger obstacles for less developed nations and SMEs than for larger companies in the Global North.

C. The Escape Valve: Opting in to Privacy Accountability

In a notable convergence around a common policy, the United States and the European Union agreed, separately and jointly, on the need to find a way a way to avoid potentially disastrous outcomes. The bad result would be world regulatory systems causing a significant blockage of global data exchanges. The result has been the creation of an escape valve in the form of accountability mechanisms. Short of a formal adequacy finding, data exporters and importers use these legal tools to demonstrate that "adequate" protection will be provided for the personal data at stake.

---

[229] *Id.*

[230] Japan amended its laws to provide special protections for data originating from the EU. *See Data Protection Laws of the World: Japan*, DLA PIPER (Jan. 1, 2022), https://perma.cc/URE6-ATYB. Currently, Israel is considering the provision of special protection for data from the European Union. For a tweet storm regarding the surrounding controversy in Israel, see Omer Tene (@omartene), TWITTER (July 7, 2022), https://perma.cc/W5CR-UPLH.

1. The model in a nutshell.

Because both the United States and the European Union have trading partners that do not follow their respective models for trade and privacy, they both provide accountability mechanisms as a private alternative to broader legal mandates. These procedures permit organizations to opt into a binding program overseen by an accountability agent. As is typical of the spaghetti bowl of trade and privacy law, there are multiple variations in the elements of accountability mechanisms.

2. Elements of an accountability model.

Privacy accountability mechanisms supply an organizationally based approach to cross-border data transfers that private and public authorities then reinforce. Kuner has explained that determinations of the permissibility of transfers can be geographically based or organizationally based.[231] The classic example of geographically based scrutiny is the European Union's top-down examination of whether a third country meets its adequacy standard. In contrast, organizationally based approaches begin with top-down approval of a set of requirements. A data processing organization can then choose to opt into these requirements and follow them regarding transferred personal data. Finally, there is typically an accountability agent that checks on whether these rules are in fact followed. We turn now to how the United States has approached the use of privacy accountability, how the European Union has done so, and how their joint use of this approach has fared.

a) The U.S. escape valve: APEC. The classic example of a U.S.-promoted accountability mechanism is the CBPR system, established in 2011 by the Asia-Pacific Economic Cooperation (APEC).[232] The initial step in the development of the APEC Data Trade Model was the APEC Privacy Framework (2005), which, like the OECD Guidelines, offers soft law—that is, an instrument that is not directly binding, but that creates expectations about future conduct. As is typical for soft law, the resulting "[o]bligations are, to a large extent, in the eye of the beholder."[233]

---

231 KUNER, *supra* note 226, at 64–76.

232 APEC, APEC CROSS-BORDER PRIVACY RULES SYSTEM 1 (updated Nov. 2019) [hereinafter CBPR], https://perma.cc/CY54-EXDX.

233 Guzman & Meyer, *supra* note 65, at 174.

The APEC Framework consists of nine principles, which are themselves based on an earlier example of privacy soft law, namely the OECD Guidelines. Both the OECD Privacy Guidelines and the APEC Privacy Framework illustrate "something more than a complete absence of commitment, but something less than full-blown international law."[234] Both are best understood in the Guzman-Meyer sense as coordinating devices. The APEC and OECD lack the power to generate hard law but can assist countries in generating a focal point where convergence on a policy solution is possible.

APEC developed the CBPR as a mechanism to harden the soft-law approach of the Privacy Principles. The CBPR explicitly states, "Nothing in this document is intended to create binding international obligations, affect existing obligations under international or domestic law, or create obligations under the laws and regulations of APEC Economies."[235] But the CBPR system permits APEC member economies to participate in a system that permits *individual companies* to agree to a binding set of rules.[236] As Guzman and Meyer pointed out, soft law should be viewed as a continuum.[237] The CBPR builds on the softer law of the APEC Privacy Principles by creating an opt in to harder rules.

The purpose of the CBPR system is to permit organizations engaged in global data trade to demonstrate their commitment to privacy and security. In setting up the CBPR, APEC member economies agreed on a formulation that lowers transaction costs for organizations by providing preapproved principles that would smooth the process of international data transfers. Yet thus far only nine of the twenty-one APEC economies have entered into the CBPR system.[238] And this step by itself creates no obligations on any company in these territories; it only opens the door for their participation in a comprehensive privacy certification system.

Companies seeking CBPR certification must apply to a recognized APEC "accountability agent." In turn, each country that

---

234 *Id.* at 180.

235 CBPR, *supra* note 232, at 1.

236 *Id.* at 4, 8.

237 Guzman & Meyer, *supra* note 65, at 173.

238 *Participation in the APEC Cross-Border Privacy Rules (CBPR) System Affords Asia-Pacific Economic Cooperation Members a Unique Opportunity to Work*, CROSS BORDER PRIV. RULES SYS., https://perma.cc/LCE8-KARD (listing the nine currently participating economies: Mexico, the United States, Canada, Japan, South Korea, Singapore, Australia, Chinese Taipei, and the Philippines).

joins the CBPR system is eligible to designate one or more organizations, often private sector entities, to fulfill this oversight role.[239] A company that intends to make use of the CBPR system must then select an accountability agent within the participating APEC economy in which it is "primarily located."[240] The agent evaluates the company according to a list of fifty privacy requirements that further operationalize the nine APEC privacy principles.[241] Companies that meet these requirements are then certified as in compliance with the CBPR.[242]

If companies fail to comply with their certification, the first step for enforcement is with the accountability agent.[243] A certification is also legally enforceable by the "Privacy Enforcement Authority" (PEA) in the economy in which the company is certified.[244] In the United States, the Federal Trade Commission is the PEA.[245]

The APEC CBPR system has been seen as setting weaker standards than those imposed by European law. Professor Lee Bygrave concluded that it offers standards that "are generally lower than those" found in European laws, and that it is "an instrument with a mild prescriptive bite."[246] Moreover, many of the framework's principles are subject to broad exceptions.[247] Thus

---

[239] CBPR, *supra* note 232, at 8–9.

[240] *Id.* at 9. In the United States, there are five approved accountability agents: TRUSTe, Schellman & Company, LLC, NCC Group, HITRUST, and BBB National Programs. Documents, *Accountability Agent Participation*, CROSS BORDER PRIV. RULES SYS., https://perma.cc/ZR72-PMDU. In addition, there are four approved accountability agents abroad: JIPDEC (Japan), Info-communications Media Development Authority (Singapore), KISA (South Korea), and Institute for Information Industry (Chinese Taipei). *Id.*

[241] *What is the APEC CBPR?*, NCC GRP., https://perma.cc/6PQ2-CCGK; *Accountability Agent APEC Recognition Application*, APEC Annex C, 12–50, https://perma.cc/6AVA-7HVV (containing a list of the questions asked by the agent).

[242] *What is the Cross-Border Privacy Rules System*, APEC (Oct. 2021), https://perma.cc/J4EC-NWJG.

[243] CBPR, *supra* note 232, at 6.

[244] *Id.*

[245] *FTC Becomes First Enforcement Authority in APEC Cross-Border Privacy Rules System*, CROSS-BORDER PRIV. RULES SYS. (Oct. 10, 2018), https://perma.cc/6Z76-8M4P.

[246] LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 76 (2014).

[247] See Ellyce R. Cooper, Alan Charles Raul & Sheri Porath Rockwell, *The Privacy, Data Protection and Cybersecurity Law Review: APEC Overview*, THE LAW REVIEWS (Oct. 26, 2021), https://perma.cc/JE35-LKY3 ("These principles are not intended to impede governmental activities within the member economies that are authorized and thus the principles allow exceptions that will be consistent with particular domestic circumstances.").

far, "the only enforcement actions taken by the FTC were against three companies falsely claiming to be CBPR certified."[248]

b) The EU escape valve: Standard Contractual Clauses and Binding Corporate Rules. Like the United States, the European Union has developed ways to permit organizations to agree to pre-negotiated binding standards for data trade to meet an acceptable level of privacy. This is necessary because, as we have seen, the European Commission has found so little of the world outside Europe to have "adequate" data protection law. As Professor Joel Reidenberg predicted in 2000, "If [EU] data protection is taken seriously, then systemic legal conflicts should cause disruption of international data flows."[249] Accountability mechanisms offer a means to avoid such disruption by permitting organizations in jurisdictions not deemed adequate to voluntarily follow EU-approved data handling practices.

The key mechanisms in this regard are the Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).[250] The SCCs simplify the process of crafting data-transfer agreements. Rather than using attorneys to draft contracts from scratch and then seek EU approval, a company can adopt the model contractual clauses and use their "off-the-rack" language, which the European Union wrote to provide "adequate" protection.[251] If there are any deviations from the exact language of the SCC, each member state from which data will be transferred must grant approval to the revised contractual agreement.

BCRs offer another mechanism by which to engage in data transfers to countries not declared adequate, but only *within* a single company or a group of affiliated companies. BCRs require that an organization promise to follow certain broadly defined procedures, cooperate with EU data protection authorities, and receive approval from a "lead" data protection authority.[252] Dr. Lothar Determann, a leading international privacy lawyer, warned, "The greatest administrative burden has been associated

---

[248] Andrei Gribakov, *Cross-Border Privacy Rules in Asia: An Overview*, LAWFARE (Jan. 3, 2019), https://perma.cc/7RV9-E7C5.

[249] Reidenberg, *Resolving*, *supra* note 10, at 1337.

[250] *Standard Contractual Clauses (SCC)*, EUR. COMM'N, https://perma.cc/N672-HJ87; *Binding Corporate Rules (BCR)*, EUR. COMM'N, https://perma.cc/G4ZU-VV2G.

[251] *Standard Contractual Clauses (SCC)*, *supra* note 250.

[252] LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO DATA PRIVACY LAW 43 (4th ed. 2020).

with implementing Binding Corporate Rules."[253] The difficulty follows because there is no official template, but only guidance as to the necessary internal corporate rules.

In its SCCs and BCRs, the European Union characteristically behaves in a rigorous fashion. The SCCs and BCRs are not lenient instruments by any stretch but rather stringent attempts, even within the context of an escape valve, to emphasize privacy over trade. The resulting frameworks are also highly intricate, with the promise of nearly limitless work for attorneys and significant compliance burdens for their clients. For example, Determann also warned that SCCs become highly complex when a data exchange involves a so-called "onward transfer," such as those involving "external service providers, business partners, [and] government agencies (e.g., in the case of investigations, litigation or reporting obligations)."[254] When such transferred information is to be shared further, it "can be difficult or impossible" for the initial transferee to use SCC terms verbatim with the onward transferee.[255] Examples include when data is sought as part of pretrial discovery, when a foreign government is carrying out an investigation, or when a company is dealing with business partners who do not wish to follow EU data protection law.[256]

The accountability mechanisms in the United States and Europe also differ in their types of oversight. As we have seen, the United States relies on a mixture of private sector and governmental oversight of the CBPR system, but there has not been a significant number of enforcement actions thus far. In Europe, in contrast, SCCs and BCRs are policed in the first instance by national Data Protection Authorities. These two mechanisms are also subject to CJEU scrutiny for their compliance with constitutional requirements for privacy. Moreover, considerable attention has been paid to the form of the SCCs and BCRs from EU institutions, including the Commission. In 2021, the Commission approved a revised set of SCCs, including the requirement of a new set of supplementary measures in response to CJEU concerns about U.S. national security surveillance.[257] The EDPB has suggested using encryption as one such supplemental measure.[258]

---

[253] *Id.*

[254] *Id.* at 44.

[255] *Id.* at 45.

[256] *Id.*

[257] *European Commission Adopts New Tools for Safe Exchanges of Personal Data*, EUR. COMM'N (June 4, 2021), https://perma.cc/LV74-ZRYC.

[258] *See Recommendations Version 2.0*, *supra* note 187, at 32.

c) The shared escape valve: The Safe Harbor, Privacy Shield, and beyond. The United States and European Union have also collaborated on common accountability mechanisms in the Safe Harbor (2000) and the Privacy Shield (2016).[259] Faced with notable differences between their two kinds of data privacy law, the European Union (acting through the Commission) and the United States (acting through the Commerce Department) negotiated the elements of these two self-certification programs.[260] These were mixtures of EU-U.S. standards with successive agreements edging closer to the EU version of data privacy norms. In each instance, however, the CJEU identified fatal constitutional flaws in the resulting mechanism and invalidated it. Nonetheless, the two jurisdictions recognize the necessity of such an escape valve, which is demonstrated by the ongoing negotiations between the Commission and the Commerce Department to devise a successor to the Privacy Shield.

How have these shared EU-U.S. escape valves functioned? The basic model was to have U.S. companies agree to follow a core set of privacy standards for personal data transferred from the European Union. Companies self-certified their adherence to the announced standards and then attested in an online public registry that they have conducted a self-assessment. Compliance with the standards was overseen by U.S. federal agencies, including the Federal Trade Commission (FTC).

In *Schrems I*, the CJEU invalidated the Safe Harbor because of two concerns. First, the agreement did not sufficiently limit the U.S. government's access to personal information transferred from the European Union. Second, the CJEU was concerned about the one-time rather than ongoing nature of the Commission's adequacy finding for the Safe Harbor. The CJEU stated, "[I]t is incumbent upon the Commission . . . to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified."[261]

---

[259] Issuance of Safe Harbor Privacy Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 45,667–45,668, (July 24, 2000); *Privacy Shield Overview*, INT'L TRADE ADMIN., https://perma.cc/UHX9-Z54T.

[260] Reidenberg, *E-Commerce*, *supra* note 10, at 738; *EU-U.S. Privacy Shield*, U.S. DEP'T OF COM., https://perma.cc/2X5B-J542.

[261] *Schrems I*, *supra* note 2, at ¶ 76.

The Privacy Shield responded to these CJEU concerns in three ways.[262] It offered concrete commitments about data privacy from the U.S. Director of National Intelligence, established a Privacy Shield Ombudsperson in the State Department to respond to EU individual complaints about national security surveillance, and created mechanisms for the Commission to review its adequacy finding.[263] The Privacy Shield survived two annual EU-U.S. joint reviews before the CJEU found that it did not supply an "essentially equivalent" level of protection for transferred data as that provided within the European Union.[264] In *Schrems II*, the EU High Court criticized a lack of limits on the scope of bulk collection of personal data, an absence of effective remedies for EU data subjects (including the inability to bring an enforcement action before an independent court), and the insufficiency of the ombudsperson mechanism.[265]

Currently, two of the world's largest economies, the United States and the European Union, are in the process of reviving and trying to live under their own tailored accountability mechanism. On March 25, 2022, the European Union and the United States announced that they had reached an accord "in principle" on a new bilateral data sharing arrangement to replace the Privacy Shield. The new agreement is termed the "Trans-Atlantic Data Privacy Framework."[266] The importance of the new accord was reflected by its proclamation in a joint press conference by President Joseph Biden and Ursula von der Leyen, the head of the Commission of the European Union.[267]

The next crucial step in the development of the Data Privacy Framework came on October 7, 2022, with the release of an executive order (EO) setting out significant privacy safeguards on U.S. signals-intelligence activities.[268] The EO permits individuals in "qualifying countries" to seek redress for unlawful U.S. surveillance from a new official, the Civil Liberties Protection Officer,

---

262 *EU-U.S. Privacy Shield Framework Principles*, U.S. DEP'T OF COM., https://perma.cc/93UE-VENA.

263 *Id.*

264 *Schrems II*, *supra* note 2, at ¶¶ 180–81, 185, 191.

265 *Id.*

266 *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, WHITE HOUSE (Mar. 25, 2022) [hereinafter *FACT SHEET*], https://perma.cc/L99J-4AU9.

267 Vincent Manancourt, *EU, US Strike Preliminary Deal to Unlock Transatlantic Data Flows*, POLITICO (Mar. 25, 2022), https://perma.cc/8NVS-42LD.

268 Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 14, 2022).

and to appeal decisions from this person to a newly created Data Protection Review Court. The EO also sets new restrictions on the bulk collection of data and limits surveillance to that which is "necessary and proportionate."[269] The concepts of necessity and proportionality are deeply engrained in the CJEU's jurisprudence.[270] The goal of the EO is to "*Schrems* proof" the Data Privacy Framework through limits on the scope of bulk collection of personal data, an increase in remedies for EU data subjects (§ 3(c) and (d)), and an enhanced status for the Civil Liberties Protection Officer beyond that previously allowed the Ombudsperson.[271]

The EO also demonstrates the European Union's importance in making data privacy for the world. The EO, while clearly designed to address European concerns about U.S. national security surveillance, does not mention the European Union. In fact, its protections for individual privacy extend far beyond the transatlantic relationship. The EO pledges that U.S. surveillance authorities will take into consideration the privacy and civil liberties of "all persons, regardless of nationality or country of residence."[272] The EO opens its recourse mechanisms to all citizens of a "qualifying state."[273] Here, it brings in a concept of reciprocity. A qualifying state is one whose laws or requirements call for "appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information."[274]

Under the EO, the Attorney General will be the key gatekeeper. The EO grants the Attorney General the power to "designate a country or regional economic integration organization as a

---

269 Press Release, *Questions & Answers: EU-U.S. Data Privacy Framework*, EUR. COMM'N (Oct. 7, 2022) [hereinafter *Questions & Answers*], https://perma.cc/Y8AL-ZEJW.

270 *See id.* (explaining that the Commission believes the CJEU will uphold the agreement because of the "necessity and proportionality" safeguard); *see also* Treaty on European Union art. 5, 1992 O.J. (C 191) ¶ 4; *Necessity and Proportionality*, EUR. DATA PROT. SUPERVISOR, https://perma.cc/7MWK-YZAN. Regarding the CJEU's use of these principles in a data protection case, see *Facebook Ireland Ltd v. Gegevnsbeschermingsautoriteit*, C-645/19 (June 15, 2021). For a discussion of the roots of these principles in Article 52(1) of the Charter of Human Rights, see EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 46–48 (2018).

271 *See also Questions & Answers*, *supra* note 269.

272 Exec. Order No. 14,086, 87 Fed. Reg. at 62,283. The EO's framing of privacy in this fashion is one already reflected in President Barack Obama's 2014 Presidential Policy Directive (PPD) 28, which regulated signals intelligence activity. PPD 28 also recognized the dignity of all persons, "regardless of their nationality or where they might reside." Press Release, Off. of the Press Sec'y, *Presidential Policy Directive—Signals Intelligence Activities (PPD-28)* (Jan. 17, 2014), https://perma.cc/4U6K-UBGF.

273 Exec. Order No. 14,086, 87 Fed. Reg. at 62,293.

274 *Id.*

qualifying state," and the Attorney General will presumably designate the European Union as such a "qualifying state."[275] But the structure of the order permits the Attorney General to open the redress mechanisms beyond the EU to the world. In contrast, the Privacy Shield was EU focused. As the Commission implementing decision for it stated, "The protection afforded to personal data by the Privacy Shield applies to any EU data subject whose personal data have been transferred from the Union to organisations in the U.S. that have self-certified their adherence to the Principles with the Department of Commerce."[276] In short, its redress mechanisms were open only to "EU data subjects." The Data Privacy Framework shows the EU reshaping U.S. international surveillance law to more closely resemble its own approach and also incentivizing other nations to follow this path.

Under the Data Privacy Framework, U.S. companies will face uncertain transaction costs due to the inevitable case to the CJEU challenging the new accord. The lead litigant in the two previous cases, Max Schrems, has already announced his readiness to take on this task if the resulting text "is not in line with EU law."[277] Schrems predicted, "We expect this to be back at the Court within months from a final decision."[278] The risk is that the Data Privacy Framework will meet the same ignoble end before the CJEU as its predecessors, the Safe Harbor and Privacy Shield.

Nonetheless, there are lessons to be drawn from this saga. The initial one is applicable for all of the accountability mechanisms surveyed. These escape valves are second-best solutions: both the European Union and United States would prefer that other jurisdictions follow their respective mixtures regarding trade and privacy. The shared solution is to allow organizations to opt in to a general set of principles and then to turn to accountability agents for oversight.

---

[275] *Id.*; *see also Questions & Answers*, *supra* note 269.

[276] Commission Implementing Decision No. 1250/2016 of 12 July 2016, art. 2(16), 2016 O.J. (C 4176) ¶ 16.

[277] Max Schrems, *"Privacy Shield 2.0"? - First Reactions by Max Schrems*, NOYB (Mar. 25, 2022), https://perma.cc/FE4M-DZKB. This initial statement was followed by an open letter from Schrems to key policymakers calling the apparent approach of Privacy Shield 2.0 "deeply concerning." Max Schrems, *Open Letter on the Future of EU-US Data Transfers*, NOYB (May 23, 2022), https://perma.cc/7G8A-Y2L9.

[278] *Id.* For a hopeful assessment of the new executive order's contribution to the Data Privacy Framework, see Kenneth Propp, Peter Swire & Théodore Christakis, *The Redress Mechanism in the Privacy Shield Successor*, IAPP PRIV. ADVISOR (Oct. 11, 2022), https://perma.cc/M8GV-F8QU.

There are also important institutional lessons from this saga. The successive escape valves between the European Union and the United States have distributed decision-making power among different institutions. In the case of the European Union, the most powerful of these has been the CJEU, which has not hesitated to void successive EU-U.S. agreements. In the case of the United States, enforcement, whether under the APEC CBPR, or the Safe Harbor and then the Privacy Shield, has proven less intense. The FTC approached its enforcement of the Privacy Shield largely as an "add-on" claim against companies that had also violated U.S. privacy law, including a claim against Cambridge Analytica, or in straightforward cases against companies that claimed on their websites to be participating in the Privacy Shield but had failed to register as required on the online public registry.[279] Here, the Data Privacy Framework may mark a major change by leading to far greater U.S. enforcement. The creation of new oversight institutions regarding signals intelligence, namely, the Civil Liberties Protection Order and the Data Protection Review Court, point to this possibility.

Additionally, a significant innovation of the Data Privacy Framework is the possible opening of an "escape valve" for the benefit of the rest of the world. The Safe Harbor and then the Privacy Shield were strictly bilateral agreements with benefits for the EU and United States alone. The EO will not only alter how signals intelligence is carried out with respect to European citizens abroad but also pledges the U.S. to follow EU concepts of "necessity and proportionality" for electronic surveillance of persons across the entire world. It also offers the possibility of nations beyond the EU of becoming "qualifying states" to gain access for their citizens to new privacy enforcement mechanisms in the United States.

Ultimately, the Transatlantic Data Framework, once enacted, will remain a distinct deal, one carefully negotiated between the European Union and the United States. It does not

---

[279] *See FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield*, FTC (Dec. 6, 2019), https://perma.cc/QT6M-VWE9; *FTC Takes Action against Companies Falsely Claiming Compliance with the EU-U.S. Privacy Shield, Other International Privacy Agreements*, FTC (June 14, 2019), https://perma.cc/RC3A-BTVR (reaching a settlement agreement with a background-screening company over allegations that it falsely claimed to be a participant in the EU-U.S. Privacy Shield and sending thirteen warning letters to other companies for falsely claiming participating in international privacy agreements).

solve the data-trade problem for states from the Global South hoping to provide services to the EU. The U.S. boasts political and economic leverage with the EU that developing states cannot hope to match.

III. TOWARDS PRIVACY AND TRADE

Privacy and free trade need not be in mortal opposition. In fact, in our view, privacy should be incorporated into an ambitious new world trade treaty. This Part develops a vision for a Global Privacy Agreement and sets out its normative foundation. We recognize that others may favor different policy approaches and therefore discuss alternative solutions to the current crisis.

A. Normative Considerations

In the scholarly literature concerning global data transfers, those who favor privacy share certain presuppositions about the underpinnings of the regime for world trade. These authors perceive a dichotomy between neoliberal free-marketers (the advocates of trade) and privacy defenders (the protectors of human rights).[280] Setting up the issue in this fashion preordains a conclusion that privacy is inevitably to be favored over trade. Yet, there are other normative visions of international trade beyond neoliberalism, and ones that will enrich the policy discussion in this area. This Section presents an interpretation of the values present in trade and in privacy and locates a shared commitment to opportunity and democratic self-rule in each.

1. The value of trade.

In a demonstration of the standard dichotomy, Yakovleva saw free trade as centered on promoting "efficiency gains" and "maximization of wealth," while data privacy rests on human dignity and autonomy.[281] In addition, its protection is "a matter of social justice."[282] While the digital single market matters, privacy "will always prevail" as a value for the European Union because of the constitutional status of data protection in the EU Charter

---

[280] Yakovleva & Irion, *Pitching Trade*, *supra* note 12, at 202 ("Numerous authors have flagged the potential of international trade law to conflict with a sovereign party's measures to protect privacy.").

[281] Yakovleva, *supra* note 201, at 496, 499.

[282] *Id.* at 502.

and other fundamental EU documents.[283] In her view, "[s]imply put, by labelling certain domestic policies such as restrictions on cross-border data flows and data localization measures as digital protectionism, it is much easier to critique them, reject them, and put competing policy interests such as privacy, data protection, or industrial policy in a subordinate position."[284]

We agree with Yakovleva that the conflict between privacy and trade raises questions about values. However, there are other principles associated with trade beyond efficiency and wealth-maximization. In particular, trade rules can support the development of human capital across the world. Cross-border trade in services means a democratization of opportunity throughout the world.[285] Here, we wish to build on the vision of Justice Louis Brandeis regarding the value of business.

While scholars are likely to remember Justice Brandeis for his pathbreaking development of privacy as a "right to be let alone," his views about business are also foundational parts of his intellectual legacy.[286] Justice Brandeis cared deeply about the relationship between economic opportunity and political freedom. As he testified before the Senate in 1913, "You can not have true American citizenship, you can not preserve political liberty, you can not secure American standards of living unless some degree of industrial liberty accompanies it."[287] Pointing to the impact of industrial democracy and using the gendered language typical of the time, Justice Brandeis argued that "the faculties of men will be liberated and developed" only if the tyranny of the "money kings" ended.[288] Justice Brandeis worried about massive concentration of wealth and warned that vast family fortunes were "inconsistent with democracy."[289] He believed that the democratization of opportunity would make for better citizens.

From today's perspective, Justice Brandeis identified a set of critical concerns about the impact of business on social structure

---

283 *Id.* at 506.

284 *Id.* at 496.

285 CHANDER, *supra* note 166, at 18–19 ("The search for talent has gone global, hurdling the barriers to labor factor mobility posed by restrictive immigration laws.").

286 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

287 Control of Corporations, Persons, and Firms Engaged in Interstate Commerce, Hearings Before the S. Comm. On Interstate Com., 62nd Cong. 1155 (1911).

288 LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 222–23 (1914).

289 *Id.* at 18.

and the need for legal attention to this area. In thinking about how individual opportunity relates to political freedom, Justice Brandeis had an unshakeable belief that free and open markets benefited democracy.[290] In a largely skeptical account of Justice Brandeis's economic assumptions, Professor Thomas McCraw nonetheless conceded that he was asking the right question: "How, in an age of big business, could the government preserve American democratic values?"[291]

Brandeisian concerns are present as well in the modern promotion of international trade.[292] Indeed, trade opens markets to broader competition. Consider the role of digital trade within the European Union. Through its "digital single market" initiative, the European Union has made it clear that removing barriers to online goods and services across Europe is about more than economic prosperity.[293] In terms that would resonate with Justice Brandeis, European Commission President Ursula von der Leyen stated, "This digital Europe should reflect the best of Europe—open, fair, diverse, democratic, and confident."[294] Fair access to data creates fair opportunity for people and organizations, "whether public or private, big or small, start up or giant."[295]

Both within the European Union and on a global scale, the issue of trade implicates distributive justice. This point is especially urgent today as the developing world seeks to enter valuable markets for digital services. The internet offers the revolutionary possibility of allowing workers in the Global South to provide services to consumers and businesses in the Global North. The promise for the Global South includes offering high value business processes, from data analysis to engineering. As one of us has written, "Services now join goods in the global

---

290 MELVIN UROFSKY, LOUIS D. BRANDEIS: A LIFE 326 (2009).

291 THOMAS K. MCCRAW, PROPHETS OF REGULATION 109 (1984). Moreover, Justice Brandeis called for legal actions to promote the right structure for business and block the worst ones, such as oligarchical financial entities swapping in shadowy high-risk instruments. *Id*. In this regard, Justice Brandeis anticipated the threat of "Too Big to Fail" investment banks and the need for the kinds of reforms expressed in the Dodd-Frank Act (2010). JEFFREY ROSEN, LOUIS D. BRANDEIS: AMERICAN PROPHET 82–84 (2016).

292 Justice Brandeis joined Holmes when he used the language of free trade in declaring his belief in the power of free speech: "[T]he ultimate good desired is better reached by free trade in ideas." Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

293 *Digital Single Market for Europe*, COUNCIL OF EU & EUR. COUNCIL, https://perma.cc/NFT4-99G4 (describing landmark data privacy features achieved through the digital single market).

294 Ursula von der Leyen, *Shaping Europe's Digital Future*, EUR. COMM'N (Feb. 19, 2020), https://perma.cc/BB23-3JG7.

295 *Id.*

marketplace, with workers in developing countries able to participate in lucrative Western markets despite immigration barriers."[296] The internet allows these workers to jump the borders dividing North and South. If we were to effectively ban the Global South from being able to access or process data about persons in the Global North, workers and companies in the Global South would be denied the opportunities that Justice Brandeis would have cheered. Banning the movement of data overseas will divide nations in the virtual world.

2. The value of privacy.

Like trade, privacy is a concept with many dimensions. In the European Union, data protection is a distinct and fundamental right protected by Article 8 of the Charter of Fundamental Rights.[297] It is also bolstered by constitutional protection for the "right to respect for . . . private life," as anchored in Article 7 of the Charter.[298] These rights matter because European data protection law seeks to prevent risks to personhood caused by the processing of personal data.[299] The German Federal Constitutional Court has played a leading role in the European conceptualization of data privacy. Its influential decisions in the *Census* case (1983) and *IT Privacy* case (2008) analyze how the processing of personal data can threaten individual decisional authority and undermine "a free democratic community based on its citizens' capacity to act and participate."[300] The result is the concept of a "right to informational self-determination," an idea that European data privacy law has adopted.[301] Here, too, a connection

---

296 CHANDER, *supra* note 166, at 2.

297 Charter, *supra* note 214, at art. 8.

298 *Id.* at art. 7.

299 Paul M. Schwartz & Karl-Nikolaus Peifer, *Structuring International Data Privacy Law*, 21 INT'L DATA PRIV. L. 1, 7 (2019) ("European data protection law is strongly anchored at the constitutional level. Its goal is to protect individuals from risks to personhood caused by the processing of personal data.").

300 Bundesverfassungsgericht [BverfG] [Federal Constitutional Court], Urteil vom. 15 Dezember 1983 - 1 BvR 209/83 [Judgment of 15 December 1983 - 1 BvR 209/83], ECLI:BVerfG:1983:rs19831215.1bvr020983 1 (Dec. 15, 1983) (*Census* Case); Bundesverfassungsgericht [BverfG] [Federal Constitutional Court], Urteil des Ersten Senats vom. 27 Februar 2008 - 1 BvR 370/07 - 1 BvR 595/07 [Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 - 1 BvR 595/07], ECLI:DE:BVerfG:2008:rs20080227.1bvr037007 1 (Feb. 27, 2008) (*IT Privacy* Case).

301 For an early analysis of the right to information self-determination, see generally Paul M. Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMPAR. L. 675 (1989). For a discussion of its influence, see Spiros Simitis, *Einleitung* (Introduction), *in*

can be made with the thought of Justice Brandeis. In the careful interpretation of Professor Neil Richards, Justice Brandeis's key contribution is a conception of privacy as protecting "individual's' emotional and intellectual processes so that they can think for themselves."[302] Privacy is about safeguarding "belief formation" and the production of a "self-governing citizenry."[303] Moreover, as this discussion shows, Yakovleva is correct to link privacy to human dignity and autonomy. But there is also much more to be said regarding privacy and how it relates to trade.

In particular, privacy and trade can serve related goals. Like privacy, trade can further democratic self-rule. Just as privacy is about self-determination, the international trade order seeks to assist global development and help empower citizens of different countries. Moreover, data privacy alone is not of unalloyed benefit to democratic community. The protection of privacy, even in the European Union, is not a one-way ratchet working in favor of restrictions on flows to personal data. As the German Federal Constitutional Court noted in its *Census* decision, "The individual does not possess any absolute, unlimited mastery on 'his' data; rather, he is a personality . . . developing with the social community."[304] In its view, individuals are "community-related and community-bound."[305]

There are multiple values present when it comes to data privacy and information flows. For example, the CJEU has decided numerous cases that explore the need for limits on data protection rights when faced with other interests.[306] These cases assess the countervailing benefits present in law enforcement access to telecommunications information,[307] the public availability of search-engine information,[308] transparency interests in access to documents held by public authorities,[309] and additional issues. When other interests collide with data protection rights, the CJEU's favored test is a proportionality analysis. Indeed, this

---

DATENSCHUTZRECHT (Data Protection Law) 167–72 (Spiros Simitis et al. eds., 2019) and Schwartz & Peifer, *supra* note 299, at 6.

302 Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1342 (2010).

303 *Id.* at 1342, 1338.

304 *Census* case, *supra* note 300, at 34.

305 *Id.*

306 For a discussion, see EUR. UNION AGENCY FOR FUNDAMENTAL RTS., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 34–502 (2018) [hereinafter Handbook].

307 *Id.* at 37–39.

308 *Id.* at 56–57.

309 *Id.* at 16, 65–67.

concept is a central one in EU law, enshrined in Article 52(1) of the Charter, which requires that limitations on its "rights and freedoms" be "[s]ubject to the principle of proportionality."[310]

Moreover, there can be privacy-against-privacy trade-offs.[311] The European Union's GDPR recognizes this issue when it comes to the age of consent for children to data processing. As this Article has discussed, the GDPR lets member states set this age between thirteen and sixteen years. In selecting an age, the member state must decide the question of "Whose privacy?" Researcher danah boyd has observed that the question of data privacy for children on the internet frequently involves conflicts among multiple interests.[312] Children are primarily concerned with privacy from their *parents* while parents are worried about privacy for their children from *outside parties*.[313] An EU member state that sets a lower age for consent does more to protect children's information seclusion as far as their parents are concerned, but less to protect children from privacy violations by third parties. The opposite result occurs in a member state that sets a higher age of consent.

3. Of privacy and bananas.

From a certain perspective, trade and privacy must always be kept apart because to do otherwise would be to subject a human right to economic considerations. We have already quoted Simitis regarding the need for data protection to continue beyond national borders.[314] In 1994, Simitis also advised, "[D]ata protection may be a subject on which you can have different answers to the various problems, but it is not a subject you can bargain

---

[310] Charter, *supra* note 214, at art. 52(1). Under the text of Article 52(1), this requirement means that "limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." *Id.* For a discussion, see HANDBOOK, *supra* note 306, at 46–48.

[311] Professor David Pozen has explored how these conflicts between different privacy interests can occur in the context of surveillance carried out by the National Security Agency in the United States. David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 233–42 (2015).

[312] DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 54–56 (2014).

[313] *Id.* at 55–56.

[314] *See* Simitis, *supra* note 217.

about."[315] More succinctly, he declared, "This is not bananas we are talking about."[316]

As it turns out, the European Union has itself over the last decade engaged in a pattern of bargaining about privacy and trade. As this Article has shown, it has employed different tactics with the United States (bilateral accountability agreements) and with Japan and South Korea (multiyear adequacy negotiations).[317] The result has been a string of policy successes for the European Union. Linking the two has not caused privacy to be subservient to trade but has led many countries to establish or strengthen their data privacy laws, often modeling them on EU models (first the Data Protection Directive or, more recently, the GDPR). Also, as noted, privacy and trade seem to have been connected, at least politically, in dealings between the European Union and Japan and then with South Korea. For example, the mutual adequacy decision between the European Union and Japan was announced on January 23, 2019, just in time for the February 1, 2019, effective date of the EU-Japan free trade agreement.[318] In the aftermath of Brexit, moreover, the European Commission's ruling finding the United Kingdom adequate for data protection purposes came within months of the conclusion of a new trade deal between the countries.[319]

To be sure, the flow of personal data across borders is different than the transportation of bananas across oceans. As Yakovleva and Irion observed, "Personal data is peculiar in the way it combines the dignity of a human being with economic properties valuable for commercial activity."[320] Bananas, after all, do not carry our likes, dislikes, or health status, and they do not reveal where we were last Saturday night. But the comparison

---

315 Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 439 (1995) (quoting Spiros Simitis, Unpublished Comments at the Annenberg Conf. on Info. Priv. and the Pub. Interest (Washington, D.C., Oct. 6, 1994)).

316 Edmund L. Andrews, *Europe and U.S. Are Still at Odds Over Privacy*, N.Y. TIMES (May 27, 1999), https://perma.cc/A836-KCF7.

317 *See FACT SHEET*, *supra* note 266; Manancourt, *supra* note 267; Schantz, *supra* note 134; *The European Union and Japan Agreed*, *supra* note 225; *see also Questions & Answers on the Adoption of the Adequacy Decision Ensuring Safe Data Flows Between the EU and the Republic of Korea*, EUR. COMM'N (Dec. 17, 2021) [hereinafter *Data Flows Between the EU and Korea*], https://perma.cc/X7KG-TWGA.

318 *See European Commission Adopts Adequacy Decision on Japan*, *supra* note 224.

319 *Data Protection: Commission Adopts Adequacy Decisions for the UK*, EUR. COMM'N (June 28, 2021), https://perma.cc/6D7B-B285.

320 Yakovleva & Irion, *Pitching Trade*, *supra* note 12, at 202.

requires more unpacking. Similar to trade in services today, trade in bananas has long raised issues of global distributive justice. At the time that Simitis made his comparison, the WTO was considering claims by ten banana-exporting Latin American nations that the European Union's import regime had improperly discriminated between countries based on colonial ties.[321] This dispute was only settled in 2009 with the European Union's reform of its import system for bananas.[322]

In fact, bananas are exactly the kind of unprocessed export that developing countries have long complained about as an example of trade injustice.[323] There is also a potential connection here with the crisis that has followed from the Privacy Bracket. Due to the regulatory thicket, the splintering of adequacy, and the harm to SMEs, data privacy law can become a hurdle to the growth of digital service industries in the developing world. In over a quarter century of its regime for international data transfers, the European Union has found only two countries in the Global South—Argentina and Uruguay—to have adequate privacy protection regimes.[324] The danger is of an international economic order where low- and middle-income countries export low- value unprocessed goods while other countries export high-value finished goods and services. Ever-increasing privacy hurdles run the risk of preserving higher value-added information-based digital services for richer countries while confining poorer countries to the sale of bananas.

We return now to the Privacy Bracket. GATS Article XIV permits countries to take steps to protect data privacy. But where such privacy measures are used to justify restrictions on trade that violate GATS obligations, this action must be "necessary" and not a fig leaf to hide economic or political motives, such as protectionism or favoritism for certain trading partners. In other words, while privacy is a fundamental right in EU law, and trade is not, a restriction on a trade measure is permissible only when privacy is the real motivation. In the language of GATS, moreover, "necessity" means that there be no less restrictive measure. Taking this language seriously means that one must

---

321 For a summary of this complex dispute, see *Lamy Hails Accord Ending Long Running Banana Dispute*, WTO (Dec. 15, 2009), https://perma.cc/RVQ7-B27S.

322 *Id.*

323 Raj Bhala, *The Bananas War*, 31 MCGEORGE L. REV. 839, 851 (2000); Ibrahim Gassama, *Good Bananas, Bad Bananas: Hard Lessons from a Soft War*, 104 AM. SOC'Y OF INT'L L. PROC. 469, 470 (2010).

324 *Adequacy Decisions*, *supra* note 128.

consider, for example, how data privacy can be enhanced by trade. Just as keeping money in the bank is generally safer than keeping it under the mattress, storing data in a world-class cloud system is often safer than keeping data on one's office computer. Moreover, a data localization requirement means that a company might have to ensure cybersecurity at multiple data centers in different countries.[325] Privacy and trade need not be in opposition to each other.

* * *

We turn now to three possible solutions to the current state of affairs and an exploration of their benefits and costs. Our goal is to present a legal map of possible resolutions of the trade versus privacy question. People may value trade and privacy differently, and while we will share our own view as to the best way to proceed, we acknowledge the validity of other preferences. In order of increasing magnitude of the institutional effort involved, this Article points to three possible solutions: muddling through without any coordinated international action; negotiating a Global Data Privacy Enforcement Treaty; or, most ambitiously, enacting a Global Data Privacy Agreement.

B. Solution 1: Muddling Through

With the Privacy Bracket still in place, nations will continue to develop their own range of bilateral and regional arrangements. A triumph of incrementalism, this approach continues the current tug-of-war between the European Union and the United States with nations forced to pick sides or to somehow straddle the two. Here are the likely results of muddling through in this context.

First, the European Union will leverage its adequacy mechanism. Some nations will follow the recent path of Japan and South Korea to seek a formal finding of adequacy from the Union. These countries will modify their laws and perhaps offer special protections for data originating in the European Union.[326] Moreover, the Data Privacy Framework points to an innovative way that the

---

[325] *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 716–17 (2015).

[326] Japan amended its laws to provide special protections for data originating from the EU. *See Data Protection Laws of the World: Japan*, DLA PIPER (Feb. 1, 2021), https://perma.cc/EW7E-EQ7A.

European Union is leveraging its adequacy mechanism. In the recently released EO from the Biden Administration, the United States reshaped its acquisition of signals intelligence around EU notions of "necessity and proportionality" and opened its new redress mechanisms up to nations that take a similar path and can therefore be considered "qualifying state[s]."[327]

It is more than likely that the Commission will continue on its path of greater rigor and more demands in terms of required changes to national laws. The risk is that such incrementalism will place formal adequacy findings out of reach for developing nations. As for the organizational mechanisms for adequacy, the SCCs and BCRs, the European Union will continue to refine and toughen them and will do so under the watchful eye of the CJEU. Overall, the result will be heightened compliance costs, which will create obstacles for less developed nations and SMEs as compared to the developed world and larger companies.

Second, the United States will seek to expand the influence of its policy emphasis of trade before privacy. It is likely to develop new global trade arrangements to further the international flow of data. As in the USMCA, the United States will seek digital trade arrangements that consider privacy in consumer protection terms and allow considerable leeway to countries to find their own path. It will promote its APEC CBPR system, its favored opt-in accountability mechanism, and seek to counterbalance the European Union's stricter SCCs and BCRs.

Third, two of the largest world economies, the United States and the European Union, will revive and try to live under their own tailored accountability mechanism. A Privacy Shield 2.0, the Data Privacy Framework, is expected by the end of 2023, and it will move the U.S. companies that choose to follow it closer to EU data protection standards. Under it, U.S. companies will face heightened compliance costs associated with signing up for a new self-certification system while awaiting the inevitable case to the CJEU challenging the new accord. The risk is that the Data Privacy Framework will meet the same ignoble end before the CJEU as its predecessors, the Safe Harbor and Privacy Shield.

Finally, the biggest cost of muddling through will be a continuing splintering of the rules for trade and privacy. We have already seen how the adequacy concept, after widespread global

---

[327] Exec. Order No. 14,086, 87 Fed. Reg. at 62,293; *see FACT SHEET: President Biden Signs Executive Order to Implement European Union-U.S. Data Privacy Framework*, WHITE HOUSE (2022), https://perma.cc/NMF5-DFG8.

adoption and adaption, now lacks any uniform meaning. There is not even shared agreement on this standard between the European Union and the United Kingdom, which departed from the Union in January 2020. Indeed, after forty-seven years of EU membership, the United Kingdom lost no time in developing its own unique variation on the adequacy mechanism.[328]

All in all, fans of data privacy might favor muddling through as a path to promoting their favored value. In this assessment, the tug-of-war between the European Union and the United States will lead to heightened influence for the former and a loss of power for the latter. In other words, there may be more Brussels Effect and less Pax Americana.[329] But while some European businesses may prosper because of protections against foreign suppliers, many more will be harmed. For many European enterprises, their own efforts to transfer data from foreign countries will be hampered by those other countries' data protection laws. Also likely is the emergence of distinct digital trade zones—one anchored by the European Union, one by the United States, and even eventually one by China. The largest companies will manage to participate in multiple such zones. But the possibility of a global internet and the fair development of a global trade in digital services will seem a distant memory.

C. Solution 2: A Global Privacy Enforcement Treaty

A more ambitious undertaking would be to negotiate a treaty focused on strengthening accountability mechanisms for cross-border data flows. As this Article has shown, accountability mechanisms are the voluntary devices that allow corporations to commit to certain data privacy rules and thereby enable data transfers between countries that have varying privacy regimes. These resulting rules include those from the European Union (including SCCs and BCRs), those from the United States (the CBPR), and those negotiated between both (the forthcoming successor to the Privacy Shield). A Global Privacy Enforcement Treaty (GPET) would seek to put international law firmly behind

---

[328] The critical U.K. policy documents regarding adequacy were released on August 26, 2021, a little less than eight weeks after the United Kingdom's own adequacy finding from the European Union. *See* U.K. Dep't for Digital, Culture, Media & Sport, *UK Approach to International Data Transfers*, UK.GOV (Aug. 26, 2021), https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers.

[329] For a masterful exploration of the influence of the European Union, see ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020).

accountability mechanisms for data protection. Such an approach avoids having to reach global agreement on substantive privacy norms but goes beyond the current muddling through approach.

A GPET would build on the current decentralized system for creating accountability mechanisms. It would advance the call of Gregory Shaffer, made over two decades ago, for mutual recognition among countries of different approaches to transatlantic governance.[330] It builds on this earlier work by strengthening the enforcement tools available should a company fail to live up to its agreements. The GPET responds to the risk that an accountability mechanism alone cannot ensure enforcement in a distant land. What if the foreign data importer falls short of its duties under the chosen mechanism, but the accountability agent fails to enforce? Or what if there is enforcement, but the importer holds no assets reachable by courts in the exporting jurisdiction? This issue is far from hypothetical. As we have noted, there is concern that the APEC CBPR system has been accompanied by a weak level of enforcement.[331] And the OECD has pointed to the challenge that privacy enforcement authorities face in addressing cross-border cases and called for a "more global and systemic approach" to enforcement cooperation.[332]

A GPET has the potential to strengthen data-privacy accountability. Under this treaty, signatory states would agree to enforce contractual safeguards created as part of foreign and international data privacy law and then voluntarily agreed to by domestic firms. The signatories would agree to collaborate on cross-border data enforcement investigations. These countries would also agree to establish and recognize accountability measures—such as accepting some foreign SCCs as a reasonable substitute, with perhaps a requirement for an additional submission for a particular jurisdiction.

In some sense, the EU-U.S. Safe Harbor and Privacy Shield have offered a version of the GPET approach, albeit on a bilateral scale. These agreements committed the FTC to enforce the Privacy Shield against companies that opted into the system. Similarly, the APEC CBPR system requires that member states have a Privacy Enforcement Authority to enforce the privacy commitment of the corporations that commit to the system.

---

330 Shaffer, *supra* note 11, at 35.

331 *See supra* Part II.C.2.a.

332 OECD, REPORT ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS 4 (2006).

This global treaty might be part of the WTO and enforced via the WTO dispute settlement process. If the United States failed to enforce accountability arrangements against a local company, for example, the European Union could bring a challenge to the WTO. If its claim were successful, the WTO could authorize the European Union to establish trade sanctions for that failure, including the suspension of data transfers to that country.

GPET would offer a number of benefits with few, if any, costs. By strengthening accountability arrangements, more countries would trust cross-border data transfers. International coordination on privacy enforcement would increase privacy compliance. Because accountability mechanisms are optional, moreover, they would impose costs only on companies that found it worthwhile to opt in. It is likely that a GPET would be especially useful to smaller, more resource-constrained businesses.

D. Solution 3: The Global Agreement on Privacy

In 2000, Reidenberg proposed a General Agreement on Information Privacy within the WTO as a way to bridge the divide among countries on issues of data privacy.[333] This treaty would establish "an institutional process of norm development designed to facilitate in the near term the coexistence of differing regimes, and over time promote harmonization of governing standards for information privacy."[334] Reidenberg did not develop this idea in any detail, however, and did not return to his proposal before his untimely death in 2021. With his writing on this topic as inspiration, we believe that it is time to revisit the idea. It is now possible to develop a vision for a Global Agreement on Privacy (GAP) with the benefit of a quarter of a century of experience with the current data trade legal regime.

The key starting point for any GAP would be to follow the architecture of the GDPR and of its predecessor, the EU Data Protection Directive. These legal instruments established a rule of "free movement of personal data" within the European Union along with strong data-privacy requirements. Similarly, under the GAP, a member state could not refuse to transfer data to another member state on data-privacy grounds unless that other state failed to meet its treaty obligations. Achieving a GAP would

---

[333] Reidenberg, *Resolving*, *supra* note 10, at 1360.

[334] *Id.*

require agreement on its core substantive privacy commitments, dispute resolution mechanism, and enforcement apparatus.

To be sure, the substantive issue is a thorny one. To return to the bananas comparison, food safety and health are promoted by recourse to international food safety standards. Phytosanitary rules supported by the WTO help assure that bananas can be grown anywhere and can be consumed safely everywhere.[335] At first glance, moreover, data privacy may seem an unlikely candidate for the development of global norms. The issue is whether a global privacy consensus will be possible. On this score, in 1997, Professor Charles Raab observed that achieving harmonization on data privacy was proving difficult even within the European Union.[336] But Reidenberg was more hopeful. Writing in 2000, Reidenberg argued that democratic states had converged on a set of "First Principles" with respect to privacy, set forth in the fair information practice principles, but they also differed significantly on questions of implementation.[337]

We believe that the potential for convergence around shared principles of fair information practices has only deepened since that time, in large part because of the efforts of the European Union.[338] Even the United States, which has famously lacked a comprehensive EU-style data protection law, now has a growing number of more comprehensive privacy statutes at the state level.[339] Most notably, California enacted the CCPA in 2018, which was amended through a state referendum in 2020.[340] The net effect, as announced by Australian privacy expert Graham Greenleaf, is a momentous one. In his view, "After 40 years, the US has a data privacy law implementing the OECD Guidelines of

---

335 The relevant WTO agreement on food safety encourages states to adopt international standards for food safety, where available, and permits nations to adopt stricter standards as long as they are scientifically justified. *Agreement on the Application of Sanitary and Phytosanitary Measures*, WTO, arts. 3.1 & 5, https://perma.cc/3ADZ-5LQV.

336 Charles D. Raab, *Privacy, Democracy, Information*, *in* THE GOVERNANCE OF CYBERSPACE 155, 165 (Brian D. Loader ed., 1997).

337 Reidenberg, *Resolving*, *supra* note 10, at 1325. Professor Colin Bennett also found some evidence of general agreement in certain European nations, Canada, and the United States around these basic principles. BENNETT, *supra* note 73, at 125–45.

338 Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 803, 809 (2020).

339 CCPA § 1798; Colorado Privacy Act, 2021 Colo. Legis. Serv. Ch. 483 (S.B. 21-190) (Effective July 1, 2023); Virginia Consumer Data Protection Act, 2021 Va. Gen. Assembly Special Session I Ch. 36 (§ 1392) (to be codified at VA. CODE Ch. 52 § 59.1).

340 Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS INST. (Nov. 17, 2020), https://perma.cc/8WT4-PTE5.

1980 for a significant part of its private sector."[341] Indeed, in his further analysis, Greenleaf observed that the CCPA "is, considered overall, a law that approximates the current international standard for data privacy laws outside Europe: inclusion of almost all the 1st generation principles of the 1980s, and about 7 of the 10 additional principles embodied in the 1995 EU Directive and Convention 108."[342]

A consensus concerning privacy law would also be politically and economically valuable and, hence, in the interests of many parties. The shared economic interests in cross-border data flows would support efforts to find a consensus. Cross-border data flows are critical, not just for U.S. big tech, but for European and other enterprises, large and small. A recent report from the Congressional Research Service points to the shared value of transatlantic data flows. Information transfers between the United States and Europe amount to more than half of Europe's data flows and about half of U.S. data flows internationally.[343] The size of trade in services related to information and communications technology was over $264 billion in 2022, with a trade surplus in this area of $82 billion in favor of the United States.[344]

While the United States often expresses concerns about data protectionism from the European Union, the European Union worries about data protectionism in foreign countries that might disadvantage commercial enterprises in its member states. Indeed, a key goal of its trade negotiations is the elimination of such barriers. As the European Commission makes clear, "When negotiating trade agreements, the EU proposes the straightforward prohibition of protectionist barriers to cross-border data flows."[345] Finally, a GAP need no more repress different cultural values than the GDPR. This latter document has set acceptable privacy rules for EU member states, including Denmark, Estonia, France, Germany, Hungary, Latvia, and Spain.

In developing its core commitments around privacy, the GAP has two paths open to it. It can develop substantive privacy commitments *internally* as part of the treaty negotiation process or

---

341 Graham Greenleaf, *California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?*, 168 PRIV. L. & BUS. INT'L. REP. 13, 4 (Dec. 2020).

342 *Id.* at 6.

343 CONG. RSCH. SERV., IF11613, U.S.-EU TRANS-ATLANTIC DATA PRIVACY FRAMEWORK 1 (2022).

344 *Id.*

345 *Digital Trade*, EUR. COMM'N, https://perma.cc/3BV7-KYS7.

set up a mechanism for establishing such substantive commitments *externally*, which it would then incorporate by reference. A potential internal process for it would be as part of the WTO's Joint Statement Initiative on E-Commerce.[346] This initiative was launched by Japanese Prime Minister Shinzo Abe at the G20 meeting in Osaka in 2019.[347] Abe proposed a system of "Data Free Flow with Trust" (DFFT), which is to be based on cybersecurity and personal data protection.[348] This process of creating the DFFT is generally called the "Osaka Track."[349]

Like this Article, the DFFT seeks to set up an overarching cross-border data flow framework. Also similar to this Article's aspirations, the DFFT aims to have the resulting data flows narrow the gap between rich and less privileged nations. More than eighty states, including the United States, the European Union, and China, have joined in negotiations as part of the Osaka Track and pledged "to achieve a high standard agreement with the participation of as many WTO Members as possible."[350] Our review of the leaked proposals reveals, however, that the current work product tracks the trade models represented in existing bilateral and regional trade agreements.[351] Unfortunately, the Osaka Track seems destined to preserve the Privacy Bracket.[352]

While we believe that the WTO should be the locus for the proposed global agreement on privacy, we do not think that it is the right institution to develop substantive global privacy norms. First, the WTO typically does not set international standards; it prefers to incorporate standards set by other expert international bodies, such as the Codex Alimentarius Commission for food safety.[353] Second, developing international standards through a

---

346 *Joint Initiative on E-commerce*, WTO, https://perma.cc/DA6Y-6VSZ.

347 *Director-General Azevêdo Joins Prime Minister Abe and Other Leaders to Launch "Osaka Track" on the Digital Economy*, WTO (June 28, 2019) [hereinafter *Director-General Azevêdo Joins Prime Minister Abe*], https://perma.cc/G9L7-EKXB.

348 Satoshi Sugiyama, *Abe Heralds Launch of 'Osaka Track' Framework for Free Cross-Border Data Flow at G20*, JAPAN TIMES (June 28, 2019), https://perma.cc/A564-8P9E; Shinzo Abe, *Defeatism About Japan Is Now Defeated* WORLD ECON. F. (Jan 23, 2019), https://perma.cc/PD6A-VHFM.

349 Sugiyama, *supra* note 348, at 1–2.

350 *Director-General Azevêdo Joins Prime Minister Abe*, *supra* note 347.

351 *See generally Consolidated Negotiating Text - December 2020*, WTO (Dec. 14, 2020), https://perma.cc/74BZ-VZUA.

352 *Id.*

353 *Understanding the WTO Agreement on Sanitary and Phytosanitary Measures*, WTO (May 1998), https://perma.cc/U49L-M2CD (noting that the Agreement on the Application of Sanitary and Phytosanitary Measures promotes international standards for food safety, including the Codex Alimentarius).

process *outside* the WTO could leverage independent expertise in order to allay existing concerns regarding the identification of privacy norms within an international trade regime.[354] As an example of these suspicions, Professor Margot Kaminski has argued that "trade is not the place . . . to negotiate privacy."[355] She worries about trade agreements "bundling issues" in a way that would deprioritize privacy while privileging access by private companies.[356] One way to respond to these concerns would be to draw on an external locus for consensus building and negotiations.

A prime candidate for such a role would be the Global Privacy Assembly (GPA). Formed in 1979, the GPA is the leading international forum for the world's privacy officials.[357] Today, some eighty-two nations participate in it, greatly increasing the GPA's representativeness since its origins as a meeting place largely for European privacy officials.[358] In short, the GPA is the international organization with the greatest institutional expertise in the area of data privacy. While the Assembly has, at least thus far, avoided issuing international instruments, in 2020, it introduced "Joint Statements" for promoting "a global regulatory environment based on commonly held principles of data protection."[359] Through its Global Frameworks and Standards Working Group, it has also begun work on established "key principles that members can agree on."[360]

---

354 The major exception to this rule is in intellectual property, where the Agreement on the Trade-Related Aspects of Intellectual Property (TRIPS) sets out substantive minimum standards for the protection of intellectual property. Catherine Field, *Negotiating for the United States*, *in* THE MAKING OF THE TRIPS AGREEMENT: PERSONAL INSIGHTS FROM THE URUGUAY ROUND NEGOTIATIONS 134 (Jayashree Watal & Antony Taubman eds., 2015). TRIPS was negotiated as part of a multiplex set of agreements, including in goods and services, with developing countries finally agreeing to TRIPS' substantive requirements in return for better access to Western markets. Mogens Peter Carl, *Evaluating the TRIPS Negotiations: A Plea for a Substantial Review of the Agreement*, *in* THE MAKING OF THE TRIPS AGREEMENT: PERSONAL INSIGHTS FROM THE URUGUAY ROUND NEGOTIATIONS 104 (Jayashree Watal & Antony Taubman eds., 2015).

355 Margot Kaminski, *Why Trade Is Not the Place for the EU to Negotiate Privacy*, INTERNET POL'Y REV. (Jan. 23, 2015), https://perma.cc/JK6N-F8DJ.

356 *Id.*

357 *See* GLOBAL PRIVACY ASSEMBLY, [hereinafter GLOBAL PRIVACY ASSEMBLY], https://perma.cc/R8M9-ZX5X. As its website states, "The Global Privacy Assembly first met in 1979 as the International Conference of Data Protection and Privacy Commissioners. The Assembly has been the premier global forum for data protection and privacy authorities for more than four decades." *Id.*

358 *Accredited Members 2021*, GLOBAL PRIVACY ASSEMBLY, https://perma.cc/YU8R-WDSY.

359 *Joint Statements*, GLOBAL PRIVACY ASSEMBLY, https://perma.cc/UXL8-47P6.

360 Denham, *supra* note 19.

The recourse to the GPA would draw on a well-established international forum for privacy authorities. In the Assembly's own words, it connects "the efforts of more than 130 data protection and privacy authorities from across the globe."[361] In our view, moving the formulation of substantive privacy rules to an international forum would reduce the power of superpower states that might be present in bilateral negotiations. An international forum allows smaller and poorer nations to unite. Moreover, the GPA can also open its ranks in developing privacy treaty standards to representatives from the Global South that are not yet official members of this global forum.[362]

With its substantive standards in place, the GAP would include a commitment that countries adopting and enforcing its international standard would be considered "adequate" to receive data from all other member states. No additional consents or other safeguards would be necessary for parties to transfer data to other countries within the framework. Privacy rules might still limit data transfers to third parties, but not simply because the entity is located in a foreign jurisdiction as long as that country has signed the GAP.

At the same time, and to account for cultural and political differences around data-privacy values, the GAP's "free flow" rule would be subject to negotiated exclusions that each country could specify in their schedules. National sensitivities around particular types of data vis-à-vis particular foreign nations will likely be the focus of such negotiated exceptions. As an example, South Korea's national security concerns with respect to the export of detailed mapping data would be an appropriate subject for an exclusion that it might wish to include in a schedule.[363]

A turn to international organizations invites the question as to the role of authoritarian regimes in those organizations. Will those organizations produce results that end up only enhancing the power of authoritarian members? The inclusion of an authoritarian state, however, does not guarantee results favorable to that state. For example, Russia was a member of the Council of

---

361 *See* GLOBAL PRIVACY ASSEMBLY, *supra* note 357.

362 Recently, Professor David Erdos suggested that the GPA may possibly play a significant role "in promoting further reflection" on the global dimensions of the "right to be forgotten" and "facilitating practical enforcement cooperation amongst like-minded supervisory authorities." David Erdos, *The "Right to be Forgotten" Beyond the EU: An Analysis of Wider G20 Regulatory Action and Potential Next Steps*, 13 J. MEDIA L. 1, 32–33 (2021).

363 Ellen Powell, *Why South Korea Refuses to Share Mapping Data with Google*, CHRISTIAN SCI. MONITOR (Nov. 18, 2016), https://perma.cc/G774-5LL4.

Europe for a quarter century before being expelled by it in the wake of the Ukrainian invasion.[364] Yet, the Council of Europe's principal judicial organ, the European Court of Human Rights, repeatedly had held Russia in violation of its human rights commitments.[365] A similar story can be told about the European Union itself, which has sought to enhance the rule of law in such former Soviet bloc countries as Hungary and Poland.[366] The far more numerous democratic nations involved in these institutions have a real chance to cabin the power of any authoritarian nation and to enhance the path to democracy in these countries.

Once substantive norms are agreed upon, the next question will be enforcement. Here is the key advantage of the WTO as an international law forum, and the reason why it is the proper forum in which to anchor the GAP. The usual reason for seeking to place a global norm within the WTO is that it offers an effective international enforcement mechanism in the form of trade sanctions against countries that fail their obligations. If a country failed to enforce international privacy rules, its trading partners could suspend personal data flows to it unless additional safeguards were met.

While no country has brought a privacy-based enforcement action during the quarter century of the WTO's existence, we believe this result follows because the Privacy Bracket lacks detailed rules on privacy. The GAP would remedy that absence and, thereby, promote enforcement actions. As is typical for international trade agreements at the WTO, it would rely on international enforcement where a country failed to enforce its substantive norms domestically.[367] The GAP should also include

---

364 *The Russian Federation is Excluded from the Council of Europe*, COUNCIL OF EUR. (Mar. 16, 2022), https://perma.cc/KU3A-X5UL.

365 For a review of these judgments, see *Press Country Profile: Russia*, EUR. CT. OF HUM. RTS., https://perma.cc/S3N7-4GEJ. Russia has snubbed a number of these judgments, however, and insisted on the supremacy of the Russian constitution. *See* Rachel M. Fleig-Goldstein, *The Russian Constitutional Court Versus the European Court of Human Rights: How the Strasbourg Court Should Respond to Russia's Refusal to Execute ECtHR Judgments*, 56 COLUM. J. TRANSNAT'L L. 172, 178 (2017).

366 In 2022, the European Commission issued a "Rule of Law" report that included specific recommendations for all twenty-seven member nations. *2022 Rule of Law Report*, EUR. COMM'N, https://perma.cc/KRU7-Z97T. For an overview, see Gabriela Baczynska, *EU Tells Hungary, Poland to Step Up Their Democracy Game*, REUTERS (July 13, 2022), https://perma.cc/XJ9Q-P484.

367 Most of the privacy enforcement would take place at the local level, not at the international level. The substantive norms would have to be enforceable in the domestic system. Only when a nation failed systematically to enforce its privacy obligations under

mechanisms for monitoring and review, including national reporting obligations and periodic reviews of the practical workings of the substantive parts of the agreement. The resulting system should include financial support for significant capacity building among poorer nations so that they are able to enforce privacy laws and thereby be full participants in the twenty-first century trade in data.

But there would also be costs to achieving a global privacy agreement. Nations would have to prove willing to compromise on certain aspects of data protection law to reach broad agreement. These compromises are already taking place, however, as the European Union has demonstrated in its widely varied approaches and substantive requirements when negotiating with Japan, the United Kingdom, or the United States.[368] The creation of the GAP would make decisions involving privacy and trade more transparent and more international.

In the last few years, of course, the WTO's crown jewel, its dispute settlement system, has been thrown into a "legal limbo" by the failure of the United States to permit the appointment of a quorum of judges to the Appellate Body.[369] Our proposal assumes that a functioning Appellate Body is restored in due course. The Biden Administration's ambassador to the WTO has said that she will work to "restore" the Appellate Body.[370] Indeed, a functioning WTO dispute settlement system is a critical part of the international economic order, as it ensures the continuing benefits of trade continue to flow, rather its erosion through protectionism followed by tit for tat retaliation. As it stands, there is no clear alternative mechanism for enforcing international obligations. To be effective without the backing of the WTO, a stand-alone privacy agreement would need to establish its own dispute settlement mechanism, including an enforcement mechanism that included the removal of access to the offending nation's data.

---

the international agreements would another member state bring a claim against it in the WTO dispute settlement system.

368 *See FACT SHEET*, *supra* note 266; Manancourt, *supra* note 267; Schantz, *supra* note 134; *The European Union and Japan Agreed*, *supra* note 225; *see also Data Flows Between the EU and Korea*, *supra* note 317.

369 William J. Davey, *WTO Dispute Settlement: Crown Jewel or Costume Jewelry?*, 21 WORLD TRADE REV. 291, 291 (2022).

370 Simon Lester, *Maria Pagan on Reforming WTO Dispute Settlement and the Appellate Body*, INT'L ECON. L. & POL'Y BLOG (Oct. 26, 2021), https://perma.cc/82JG-HREA.

The benefits of a global privacy treaty agreement are legion. Rather than having to hire lawyers or build out data infrastructures in multiple jurisdictions, a small business could bind itself to the GAP's substantive norms and supply the world with its services and goods. The manifold benefits of a global internet would be preserved against the splintering that this Article has cataloged and analyzed.

CONCLUSION

The promise of the internet is to heighten equality across the world by permitting individuals and businesses to engage with each other in ways that border controls and immigration rules had made impossible for centuries past. The promise of global privacy law is to protect personal information as it moves from country to country. And the promise of trade is to allow anyone to benefit from new opportunities on the digital frontier by selling and buying goods and services across the world. Remarkably, the internet, modern trade law, and contemporary privacy law were formed simultaneously in the 1990s with an awareness of these future prizes. But rather than coming closer to fruition, these promises are receding as privacy and trade come into increasing conflict. Political commentator Thomas Friedman once famously claimed that the "world is flat."[371] In his view, the internet was equalizing access for business across the world, including in the Global South.[372] But the regulatory thicket created by global privacy rules means that this aspiration is increasingly remote.

This Article sounds the alarm regarding the current crisis and charts an ambitious agenda to fortify both privacy and trade. It proposes a Global Privacy Agreement that will be negotiated, like GATS, within the World Trade Organization, but with its substantive privacy norms developed within an expert institution, such as the Global Privacy Assembly. By drawing on such external expertise, a new privacy trade agreement will be responsive to concerns regarding the deprioritization of privacy. This Article sets out a path to promote self-determination and economic opportunity as part of an advancement of privacy *and* trade.

---

[371] *See generally* THOMAS FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY (2007).

[372] *Id.* at 7–8 (using a catchphrase from Indian business-processing-outsourcing pioneer Nandan Nilekani to argue that the internet equalized access to businesses around the world).

APPENDIX A: SUPRANATIONAL, NATIONAL & TERRITORIAL LAWS WITH AN ADEQUACY-TYPE STANDARD FOR DATA EXPORTS

Country	Provision
Andorra	Qualified Act 15/2003 of 18 December of personal data protection, Dec. 18, 2003, ch. VI, art. 35 ("level of data protection equivalent, at least, to that established in this Law").
Angola	Lei No. 22/2011 Ante-Projecto de Lei da Proteção de Dados Pessoais, 2011, sec. VI, art. 33 ("ensure an adequate level of protection").
Argentina	Law No. 25.326, Oct. 4, 2000, ch. II, art. 12 ("adequate levels of protection").
Australia	Privacy Act of 1988 s 1, pt 3 (Austl.) ("at least substantially similar to the way in which the Australian Privacy Principles protect the information").
Bahrain	Law No. 30 of 2018 with Respect to Personal Data Protection Law, Jul. 12, 2018, sec. 3, art. 12 ("provide adequate legislative and regulatory protection for personal data").
Benin	Law No. 2009-09 of May 22, 2009 Dealing with the Protection of Personally Identifiable Information (PII) in the Republic of Benin, ch. II, art. 9 ("sufficient degree of privacy, liberty and unalienable rights protection").
Bermuda	Personal Information Protection Act of 2016, Jul. 27, 2016, pt. 2, sec. 15(3) ("When assessing the level of protection in subsection (2) . . . the Minister, on the recommendation of the Commissioner, may designate any jurisdiction as providing a comparable level of protection for the purposes of this section.").
Botswana	Data Protection Act, Aug. 3, 2018, pt. VIII, sec. 49(1) ("the transfer of personal data that is undergoing processing or intended processing, to a third country may only take place if the third country to which the data is transferred ensures an adequate level of protection").

Brazil	Lei No. 13.709, de 14 de Agosto de 2018, ch. V, arts. 33–34; ("degree of protection of personal data adequate to the provisions of this Law").
Cabo Verde	Law No. 41/VIII/2013, Sep. 17, 2013, ch. I, arts. 19–20 ("ensures an adequate level of protection").
Cayman Islands	The Data Protection Law, 2017, sch I, pt. 1, princ. 8 ("Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects").
Chile (2017 draft)	Law No. 001-365, 2017, tit. V, art. 27 ("adequate levels of data protection").
China	Personal Information Protection Law of the People's Republic of China, Aug. 20, 2021, ch. III, art. 38 ("Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out").
Colombia	L. 1581, Oct. 17, 2012, tit. VIII, art. 26 ("adequate levels of data protection").
Dubai	Data Protection Law 2020, Jul. 1, 2020, pt. 4, sec. 26(a)(1) ("an adequate level of protection".
Ecuador	Ley Orgánica de Protección de Datos Personales, Quinto Suplemento del Registro Oficial, May 26, 2021, ch. IX, art. 56 ("provide adequate levels of protection").
Egypt	Law No. 151 of 2020 (Promulgating the Personal Data Protection Law), July 13, 2020, ch. 7, art. 14 ("Transfer of Personal Data . . . may only be undertaken if the level of data protection or security in the foreign country meets (or exceeds) the requirements stipulated under this Law, and subject to obtaining a relevant License or Permit from the Center").
European Union	General Data Protection Regulation, Apr. 27, 2016, ch. V, art. 45 ("a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that

	the third country, a territory or one or more specified sectors within the third country, or the international organisation in question ensures an adequate level of protection").
Gabon	Loi no. 001/2011 relative à la protection des données à caractère personnel, JOURNAL OFFICIEL DE LA REPUBLIQUE GABONAISE, Oct. 31, 2011, ch. VI, sec. II, art. 94 ("controller cannot transfer personal data to another State only if this State ensures a sufficient level of privacy protection, fundamental rights and freedoms").
Guernsey	The Data Protection (Bailiwick of Guernsey) Law, Apr. 26, 2017, sec. 57(1) ("A controller or processor may transfer personal data to a person in an unauthorised jurisdiction if the Authority has [generally or] specifically authorised the transfer").
Honduras (2018 draft)	Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data de Honduras, 2018, tit. IX, art. 40 ("adequate levels of treatment and protection").
Hong Kong	Personal Data (Privacy) Ordinance, No. 343, 1996, pt. 6, sec. 33(3) ("reasonable grounds for believing that there is in force in a place outside Hong Kong any law which is substantially similar to, or serves the same purposes as, this Ordinance").
Iceland	Decision of the EEA Joint Committee No. 154/2018 of 6 July 2018 ("[the General Data Protection Regulation] is to be incorporated into the EEA Agreement").
India (2019 draft)	The Personal Data Protection Act, 2019, No. 373, ch. VII, sec. 34(1)(b)(i) ("adequate level of protection").
Israel	Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001, June 17, 2001 ("a person shall not transfer, nor shall he enable, the transfer abroad of data from databases in Israel, unless the law of the country to which the data is transferred ensures a level of protection no lesser, mutatis mutandis,

	than the level of protection of data provided for by Israeli law").
Japan	Amended Act on the Protection of Personal Information (Act No, 57 of 2003 as amended in 2020), art. 28 ("foreign country establishing a personal information protection system recognized to have equivalent standards").
Jersey	Data Protection (Jersey) Law 2018, Feb. 16, 2018, pt. 8, sec. 66(1) ("ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data").
Kazakhstan	The Law of the Republic of Kazakhstan No. 94-V, May 21, 2013, ch. 2, art. 16 ("ensuring of protection of personal . . . in accordance with this Law").
Kenya	The Data Protection Act, KENYA GAZETTE SUPPLEMENT NO. 181, 2019, sec. IV, para. 48(b) ("the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws").
Kyrgyzstan	Law N 58, Feb. 21, 2008, ch. IV; art. 25(1) ("It takes into account the personal data of the recipient party in accordance with the contract protection and protection at the appropriate level established in the Kyrgyz Republic").
Lesotho	The Data Protection Act, LESOTHO GOVERNMENT GAZETTE NO. 19, 2011, pt. IV, sec. 52 ("are substantially similar to the information protection principles under this Act").
Liechtenstein	Data Protection Act of 4 October 2018, sec. V, art. 85(c) ("the adequacy decisions issued by the EU Commission…shall apply to the Principality of Liechtenstein").
Macao	Act 8/2005 Personal Data Protection Act, Aug. 10, 2005, ch. V, art. 19(1) ("provided the legal system in the destination to which they are transferred ensures an adequate level of protection").

Madagascar	Loi No. 2014 – 038 Sur la protection des données à caractère personnel, Dec. 16, 2004, ch. III, art. 20 ("only if the recipient state has legislation ensuring a level protection of persons similar to that provided by this law").
Malaysia	Personal Data Protection Act, 2010, pt. X, sec. 129 ("adequate level of protection . . . at least equivalent to the level of protection afforded by this Act").
Mali	Loi 2013-15 du 21 mai 2013 Portant Protection des Donnes a Caractere Personnel en Republique du Mali, May 9, 2013, sec. 4, art. 11 ("sufficient level of personal protection").
Monaco	Law No. 1.353 of December 4, 2008 relating to the protection of personal information, Apr. 1, 2009, ch. III, art. 20 ("relative to the protection of provided that the country or organization to which the transfer takes place has a level of adequate protection").
Montenegro	Personal Data Protection Law, Official Gazette of Montenegro 79/08, 70/09, ch. IV, art. 41 ("The adequacy of the measures of protection referred to in paragraph 1 of this Article shall be assessed in the light of all the circumstances surrounding a data transfer.").
Morocco	Loi no. 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, Feb. 18, 2009, ch. V, art. 43 ("ensures a sufficient level of protection of privacy and fundamental rights and freedoms of individuals").
New Zealand	Privacy Act 2020, pt. 8, sec. 193 ("comparable safeguards to those in this Act").
Nigeria	Data Protection Regulation, 2019, pt. 2, 2.11 ("ensures an adequate level of protection").
North Macedonia	Law on Personal Data Protection, 2020, ch. V, art. 49 ("A transfer of personal data to a third country or an international organisation may take place where the Agency has decided that the third country or the international organisation in question ensures an adequate level of protection.").

Norway	Norwegian Personal Data Act, July 10, 2018, sec. 13 ("adopt regulations regarding the transfer of personal data to third countries or international organizations").
Pakistan (Cabinet approved, awaiting legislative consideration)	Personal Data Protection Bill, 2021, sec. 14 ("data protection at least equivalent to the protection provided under this Act").
Panama	Ley 81-2019 Sobre Proteccion de Datos Personales, Mar. 26, 2019, ch. III, art. 33 ("equivalent or superior level of protection").
Paraguay (2021 draft)	Proyecto de Ley de Protección de Datos Personales en Paraguay, Apr. 30, 2021, tit. VII, art. 57 ("adequate level of protection").
Peru	Data Protection Law, June 9, 2010, tit. I, art. 11 ("sufficient level of protection").
Quebec (Canada)	Bill 64: An Act to modernize legislative provisions as regards the protection of personal information, Sept. 22, 2021, sec. 70.1 ("[B]efore releasing personal information outside Québec, a public body must conduct a privacy assessment . . . the information may be released if the assessment establishes that it would receive adequate protection.").
Russia	Federal Law of the Russian Federation on Personal Data, Jul. 27, 2006, ch. 2, art. 12 ("foreign states providing adequate protection").
Sao Tomé and Principe	Lei no. 03/2016 Visa Garantir e Proteger os dados pessoais das Pessoas Singulares, May 10, 2016, ch. V, art. 19 ("ensure an adequate level of protection").
Saudi Arabia (implementation set to begin in March 2023)	Personal Data Protection Law, Sept. 15, 2021, ch. VII, art. 30 ("countries that provide adequate level of protection").
Serbia	Zakon o Zaštiti Podataka o Ličnosti, 2008, OFFICIAL GAZETTE OF THE REPUBLIC OF SERBAI No. 97/08, ch. VIII, art. 53 ("Data may be transferred from the Republic of Serbia to a state not signatory to the Convention, or international organisation, if in this state or international organisation regulations or contract on transfer provide for a

	level of data protection in accordance with the Convention.").
Singapore	Personal Data Protection Act 2012, 2020, pt. VI, sec. 26 ("standard of protection to personal data . . . comparable to the protection under this Act").
South Africa	Protection of Personal Information Act No. 4 of 2013, ch. 9, sec. 72(1)(a) ("adequate level of protection").
Sri Lanka	Personal Data Protection Act, No. 9 of 2022, 1 THE GAZETTE OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA, part III, sec. 26(1) ("pursuant to an adequacy decision").
Switzerland (in the process of implementation, awaiting enactment of supporting ordinances)	Revised Federal Act on Data Protection, Sept. 25, 2020, sec. 3, art. 16 ("adequate level of protection").
Taiwan	Personal Data Protection Act, Dec. 30, 2015, ch. III, art. 21 ("[T]he central government authority in charge of the industry concerned may impose restrictions on such transfer . . . where the country receiving the personal data lacks proper regulations on protection of personal data").
Tajikistan	Law on the Protection of Personal Data, 2018, ch. III, art. 18 ("Transboundary transfer of personal data to the territory of foreign states, which ensures equal protection of the rights of personal data subjects, shall be carried out in accordance with this Law.").
Thailand	B.E. 2562 (2019), Personal Data Protection Act, May 27, 2019, pt. 3, sec. 28 ("[T]he destination country or international organization that receives such Personal Data shall have adequate data protection standard.").
Trinidad and Tobago	Act No. 13 of 2011, Protection of Personal Privacy and Information Act, June 22, 2011, pt. III, sec. 72(4)(b) ("[N]ot satisfied that the jurisdiction to which the information is being sent has comparable safeguards, the organization shall refer the matter to the Commissioner for a determination as to whether the other jurisdiction has comparable safeguards as

	provided by this Act and inform the individual.").
Tunisia	Organic Act no. 2004-63 of July 27th 2004 on the protection of personal data, 2004, ch. IV, art. 47 ("can only take place if this country ensures an adequate level of protection assessed with regard to all the elements relating to the nature of the data to transfer").
Turkey	Law on Protection of Personal Data No. 6698, 2016, ch. II, art. 9 ("countries where sufficient level of protection is provided").
Uganda	The Data Protection and Privacy Act 2019, Feb. 25, 2019, pt. III, para. 19 ("the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided by for this Act").
Ukraine	On Personal Data Protection, 2010, OFFICIAL BULLETIN OF THE VERKHOVNA RADA OF UKRAINE (BVR), NO. 34, ART. 481, art. 29 ("only if the relevant state provides adequate protection of personal data in cases established by law or international treaty of Ukraine").
United Arab Emirates	Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, arts. 22–23 ("Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is an Adequate Level of Protection")
United Arab Emirates, Abu Dhabi Global Market	Data Protection Regulations, 2021, pt. 4, sec. 41 ("A transfer of Personal Data outside of ADGM or to an International Organisation may take place where the Commissioner of Data Protection has decided that the receiving jurisdiction, one or more specified sectors within that jurisdiction, or the International Organisation in question ensures an adequate level of protection of Personal Data.").
United Kingdom	Data Protection Act, 2018, c. 5, para. 73 ("based on an adequacy decision").
Uruguay	Ley No. 18331 Ley de Proteccion de Datos Personales, Aug. 18, 2008, ch. IV, art. 23 ("adequate levels of protection").

Uzbekistan	Law of the Republic of Uzbekistan on Personal Data, Oct. 1, 2019, ch. III, art. 15 ("Cross-border transfer of personal data is carried out on the territory of foreign states that provide adequate protection of the rights of subjects of personal data.").
Zambia	The Data Protection Act of 2021, pt. X, § 71(2) ("The Minister may . . . prescribe the criteria for cross border data transfers . . . where the Minister considers that —(a) the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and (b) the enforcement of data protection laws by authorities with appropriate jurisdiction is effective.").
Zimbabwe	Data Protection Act 5 of 2021, pt. VIII, sec. 28 ("[A] data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient.").

APPENDIX B: AGE OF CONSENT FOR DATA PROCESSING

Location	Age	Source
Brazil	18	Lei No. 13.709, de 14 de Agosto de 2018 [Law No. 13,709, Aug. 14, 2018] (General Personal Data Protection Act "LGPD"); *see* Ana Carolina Cagnoni, *How Brazil regulates children's privacy and what to expect under the new data protection law*, IAPP (Oct. 29, 2019), https://iapp.org/news/a/how-brazil-regulates-childrens-privacy-and-what-to-expect-under-the-new-data-protection-law/.
California	13	CAL. CIV. CODE § 1798.100.
China	14	Information Security Technology—Personal Information (PI) security Specification] (effective Oct. 01, 2020), Mar. 6, 2020, at sec. 3.2.
European Union	13–16	Article 8(1) of the GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119).
India	18	The Personal Data Protection Act, 2019 (draft).
Japan	15	Amended Act on the Protection of Personal Information, Law No. 57 of 2003 as amended in 2015.