California Law Review

Volume 105 | Issue 5 Article 5

10-1-2017

Transborder Data Privacy as Trade

Margaret Byrne Sedgewick

Recommended Citation

Margaret Byrne Sedgewick, *Transborder Data Privacy as Trade*, 105 Calif. L. Rev. 1513 (2017).

Link to publisher version (DOI)

http://dx.doi.org/10.15779/Z382V2C94C

Transborder Data Privacy as Trade

Margaret Byrne Sedgewick*

Data flows continuously across national boundaries. The current model of regulation for data privacy, an essential component for safe data flow, relies impractically on jurisdiction-specific rules. This practice impedes the benefits of data, which are increasingly a necessary and integral part of day-to-day life. A look at the history of data privacy reveals that this practice is rooted in an ill-fitting adoption of privacy standards set in the period after World War II. Europe was reeling from the Nazi regime and intent on keeping the government out of the home and personal communication. Analogies between these traditional protected areas and the contemporary transmissions and use of personal data are unsatisfying—and lead to unsatisfying policy. Traditional privacy jurisprudence must be better reconciled with rapidly advancing technology and globalization.

This Note proposes reframing transborder data privacy as trade. This step would transition the regulatory model away from a jurisdiction-specific set of rules to an internationally shared set of standards that better reflects the immediate mobility of data in the cloud. The U.S. and European systems, while formally divergent enough to cause these problems, are in fact grounded in common principles that would serve as a base for an international agreement on transborder data privacy. Though political opposition to shared standards may be currently insurmountable, this Note nonetheless concludes that an international trade framework would more effectively harness the benefits and mitigate the risks of transborder data flow.

DOI: https://dx.doi.org/10.15779/Z382V2C94C

* J.D., University of California, Berkeley, School of Law, 2016. I sincerely thank Professors Saira Mohamed and Kenneth Bamberger for their encouragement and guidance with this project. I also am grateful for the keen editorial eyes of the *California Law Review* and the support of my family.

INTRODUCTION

This Note argues that data privacy, currently regulated under outdated, geographically specific privacy regulations, could be productively reconceived in an international trade framework. The law has not kept pace with advances in technology, and the current approach is poorly matched to transborder data flow, which occurs in the digital cloud and gains value through its unprecedented mobility and accessibility. Now, the Internet has "become today's global trade route," and the flow of personal data drives this economy.[1] The United States and Europe account for 30 percent of world trade, and, according to estimates from the European Commission, over half of the U.S.-EU cross border trade in services depends on an online connection.[2] In 2014 alone, the United States

1. JULIE BRILL, FED. TRADE COMM'N, GLOBAL REGULATION OF DATA FLOWS IN A POST-SNOWDEN WORLD 1 (2015), https://www.ftc.gov/public-statements/2015/02/global-regulation-data-flows-post-snowden-world-killingstad-global [https://perma.cc/KVK8-7ML5].

2. Ioanna Tourkochoriti, *The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection*, 36 UALR L. REV. 161, 161–62 (2014).

exported approximately $360 billion in digital services.[3] Despite the prominence of this global digital economy, however, transborder data flow remains primarily governed by domestic data privacy regulations that vary between states.

International trade law, which regulates cross border movement of goods and services, offers an alternative framework for transborder data privacy. Indeed, digital privacy raises international trade considerations, to which scholars have not given much attention. This Note attempts to fill in that gap and explore ways in which a trade framework could help to allow the efficient flow of data while protecting privacy and other important countervailing interests. Part I begins by providing background on traditional data privacy frameworks, introducing the existing legal instruments of data privacy regulation. This Part also identifies values and fears that the U.S. and European frameworks share, questioning the notion that the two regulatory systems are irreconcilably different. Part II frames digital privacy as a trade issue, introducing the trade law toolbox and the booming market for transborder data flow. Part III identifies key benefits of regulating data privacy in trade, including clarity and uniformity, greater attention to consumers' privacy expectations, and deeper consideration of trade benefits and common interests. Even if political opposition to shared standards are currently insurmountable, this Note nonetheless concludes that an international trade framework would more effectively harness the benefits and mitigate the risks of transborder data flow.

I.
AGREEMENT AND DIVERGENCE IN U.S. AND EUROPEAN DATA PRIVACY FRAMEWORKS

"Data privacy" typically denotes personal information control and is derivative of one's right to privacy in terms of non-interference in one's home, communications, and thought.[4] Data privacy addresses the ways in which individuals struggle to determine how their data is used, as technology has increased capacity to link data to an individual.[5] Database security breaches pose an additional malicious use of personal data, even when the data is given with consent for a specific purpose.[6]

---

3. BRILL, *supra* note 1, at 1.

4. LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 28 (2014).

5. CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 4 (2013).

6. Some data privacy advocates have suggested that all data should be treated as personal and subject to information privacy framework. Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, 00909/10/EN WP 171 (June 22, 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf [https://perma.cc/B3XP-XQ9P] (the document does not qualify "information" according to identifiability); Diane A. MacDonald & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUS. J. INT'L L. 625, 651 (2014) (arguing that data should be treated with utmost confidentiality because it "reveals the most intimate details of an individual's life"). *But see generally Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012) 0011 (Dec. 17, 2012)

Data privacy is a global issue, but there is no international instrument that regulates data privacy or mitigates differences between states' varying regulatory frameworks. The United States and the European Union (EU) are two of the most dominant actors in the regulation of privacy in transborder data flow because of the size and technological sophistication of their economies. Yet, conflict stemming from differences between U.S. and European models of data privacy impedes trade of data and diminishes data's social benefits.

Reframing transborder data flow as a trade issue would allow for resolution and a more efficient exchange. This Part introduces the existing international and regional privacy instruments that shape data flow between the United States and Europe. Despite the lack of a shared regulatory framework, this Part identifies points of commonality and consensus between the United States and Europe about what an effective privacy framework should entail. In doing so, this Part identifies ways in which greater unification would enable better data flow to achieve the benefits of big data.

A. Instruments

Data privacy law in both the United States and Europe is a relatively new field that grew out of preexisting privacy doctrine. The binding and non-binding instruments of data privacy regulation reflect this evolution. In Europe, privacy emerged as a fundamental right after World War II. As such, data privacy practices have been less flexible in the face of countervailing interests than have those in the United States.[7] The U.S. constitutional right to privacy is part of a penumbra of rights in different areas, which, broadly defined, is meant to keep the government out of personal decisions and activity.[8]

The traditional model is outdated. In emphasizing governmental abuse of privacy, the model fails to adequately acknowledge the risk to individuals from companies' collection, control, and use of personal data. A focus on trade would better serve this new, commercial use of individual data. This Section describes the demand and utility in reframing this debate as a trade issue, despite the distrust and fear between the United States and the EU of each other's regulatory system.

(Rapporteur: Jan Phillip Albrecht) (distinguishes restrictions according to identifiability); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011) (arguing for privacy rights to attach when data pertains to a particular person, while allowing generalized data to be accessible).

7. The United States, for example, took out a reservation to Article 4 of the International Covenant on Civil and Political rights (ICCPR), permitting itself to derogate from certain "essential" rights in times of national emergency. U.S. SENATE COMM. ON FOREIGN RELATIONS REPORT, 31 I.L.M. 645, 645 (1992).

8. *See generally* Lawrence v. Texas, 539 U.S. 558 (2003) (right to privacy as the basis for holding anti-sodomy laws unconstitutional); Griswold v. Connecticut, 381 U.S. 479 (1965) (right to privacy as basis for invalidating state law that prohibited the use of contraception).

1. Binding Agreements

Binding international privacy agreements describe privacy broadly as a fundamental human right. Foundational agreements, such as the 1950 European Convention of Human Rights (ECHR),[9] were drafted in response to the political abuses of World War II.[10] The ECHR protects privacy, giving binding authority in Europe to the non-binding 1948 Universal Declaration of Human Rights (UDHR), a United Nations General Assembly resolution articulating shared aspirational standards.[11] Sixteen years later, the 1966 International Covenant on Civil and Political Rights (ICCPR) expanded binding privacy protection around the world, using language almost identical to the UDHR.[12] The ICCPR is an international treaty to which 168 countries are parties, including the United States and European Union member states.[13]

The application of existing historic privacy obligations to data privacy has been ex post facto, occurring as new technologies and the corresponding proliferation of threats to individual privacy have emerged. Scholars have suggested that the drafters and original signatories to the ECHR and ICCPR (as well as the foundational, non-binding UDHR, noted above) were unaware that the privacy protection in these documents "would open the door for the protection of further aspects of privacy not mentioned or not even imagined in the codification process."[14]

Instead, the expansion of foundational privacy protections to include data privacy has evolved over time. The creation of data privacy law "engendered greater readiness to construe treaty provisions on the right to privacy as containing data privacy guarantees."[15] Significantly, this willingness to expand traditional privacy guarantees to data reflects the public's fear of the government gathering information that could be used to subject the public to excessive control, similar to the fear of governments following World War II.[16] But, with

9. European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR] (codifying the right to respect for "[an individual's] private and family life, his home and his correspondence" and prohibiting "interference by a public authority with the exercise of this right," with exceptions such as law enforcement and national security).

10. 1 COUNCIL OF EUROPE, COLLECTED EDITION OF THE "TRAVAUX PRÉPARATOIRES" 46, 62, 104 (Martinus Nijhoff ed., 1975).

11. G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

12. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, S. Exec. Doc. E, 95-2 (1989), 999 U.N.T.S. 171 (providing that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" and, second, that "[e]veryone has the right to the protection of the law against such interference or attacks").

13. *Id.*

14. Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441, 457 (2014).

15. BYGRAVE, *supra* note 4, at 15.

16. *Id.* at 21. Bygrave notes that despite its origin in foundational human rights documents, data privacy has not spurred a global movement like human rights (or the environmental, feminist, and

advances in technology and the rising value of transborder data flow, the international business of data gathering, storage, and processing makes individuals vulnerable to exploitation for profit in the private sector beyond invasions from their own government.[17]

a. European Regional Agreements

While there is no binding international instrument for data privacy protection, Europe has led the world in creating a regional approach to cross border data privacy regulation. The EU approach is defined by the European understanding of data privacy as a fundamental right.[18] In addition to the ECHR, the right to personal data protection is recognized in the Charter of Fundamental Rights of the European Union[19] and the Treaty on the Functioning of the European Union (TFEU).[20] The central implementing law to regulate data privacy in Europe from 1995 to the present[21] has been the European Commission's Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the Directive).[22] The Directive sets uniform data privacy standards and requires individual European countries to achieve and maintain those standards with

consumer protection fields). Rather, those advocating for greater protections are a smaller, elite group. *Id.* at 20–21.

17. Tension certainly exists in the public sector with high stakes between data privacy and national security and international law issues. While the focus of this Note is on private trade transactions, governmental use of data for national security and law enforcement has been the subject of a large body of research. *See* MacDonald & Streatfeild, *supra* note 6, at 651 (citing Wei Wang, *On the Relationship Between Market Access and National Treatment Under the GATS*, 46 INT'L L. 1045, 1065 (2012) ("The complicated relationship between market access and national treatment under the GATS is a reflection of the complicated issue of the separation of powers between Members and the WTO, and . . . between national law and international law.")).

18. The European Commission promoted the rollout of data privacy reform legislation in 2012 "to protect the fundamental rights and freedoms of natural persons, and in particular the right to data protection, as well as the free flow of data." European Commission Press Release IP/12/46, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [https://perma.cc/G5QH-2H4W].

19. Charter of Fundamental Rights of the European Union, Mar. 30, 2010, art. 8, 2010 O.J. (C 83) 389 [hereinafter Charter of Fundamental Rights]. First proclaimed in 2000, the Charter gained binding force with the Treaty of Lisbon in 2009. *Id.* at 403 (article 8). Article 8 "Protection of personal data" addresses the right to data privacy. *See id.*

20. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU].

21. Significantly, the EU Parliament approved the EU General Data Protection Regulation ("GDPR") in April 2016, and the law will become effective May 25, 2018. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]; *see* discussion *infra*.

22. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter The Directive]. The bill was enacted sixteen years after the European Parliament demanded a regulation to restrict personal data processing. Spiros Simitis, *Foreword* to PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION, at v (1996).

domestic measures.[23] In particular, the Directive serves three enumerated objectives: to ensure the rights of individuals, to promote free circulation of data in the EU through harmonized protection, and to prevent abuse in non-EU countries of data originating in the EU.[24] This third objective, governed by Articles 25 and 26, has been the main point of tension with U.S. businesses that want more freedom in transborder data flow.

Article 26 requires that data use have unambiguous consent from the data subject or be legitimated by the data being "necessary for the performance of the contract," such as transferring money to a foreign bank, making a hotel reservation, booking travel, or concluding an employment or insurance contract.[25] Consent is a requirement common in the U.S. and EU law, reflecting a shared concern that the protective rules not be too paternalistic or rigid.[26] However, consent requirements also raise similar problems in both frameworks.[27]

Article 25 establishes a qualified prohibition on the transfer of personal data to non-European countries that fail to "ensure an adequate level of protection."[28] This adequacy standard has become a model and the dominant rule in transborder data flow. In the EU, officials determine adequacy based on country-specific assessments. Third party measures must adhere to EU core principles, which Paul Schwartz and Joel Reidenberg define as:

> the deliberate limitation of the use of personal data to cases explicitly acknowledged by mandatory rules, the restriction of the processing to the data needed for a purpose clearly defined in advance and known to the data subject, the transparency of the processing, the guarantee of a series of rights securing the access of the data subjects to the information concerning them as well as their ability to demand and obtain the necessary corrections, and the establishment of an independent control authority.[29]

---

23. *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [https://perma.cc/ED5L-DZRK] (upholding the "right to be forgotten").

24. SCHWARTZ & REIDENBERG, *supra* note 22, at v.

25. *Id.* at vii.

26. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 6 (1966) (casting privacy as individual control over personal information).

27. *See* OMER TENE & CHRISTOPHER WOLF, FUTURE OF PRIVACY FORUM, THE DRAFT EU GENERAL DATA PROTECTION REGULATION: COSTS AND PARADOXES OF EXPLICIT CONSENT 3–4 (2013), http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Consent-January-201310.pdf [https://perma.cc/6FAW-WXHC] (arguing that policy makers have accepted Westin's thesis as gospel, creating a burden on individuals and notice fatigue); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1247 (2013) (arguing that, even where a consumer gives her consent, limited competition in the market creates a power imbalance which can further constrain actual individual choice).

28. The Directive, *supra* note 22, art. 25.

29. SCHWARTZ & REIDENBERG, *supra* note 22, at ix.

Beyond this requirement, third-party measures need not be identical to any one European law—and the measures could be comprised of statutes, court decisions, professional rules, or private party contract terms that, in aggregate, establish the country's de jure and de facto privacy framework.

The adequacy standard has proven to be both too exclusive and too flexible.[30] Due to the difficulty of assessing an entire country's de jure and de facto privacy framework, critics have argued that the adequacy standard does not meaningfully distinguish between robust and non-robust domestic measures. For example, Omer Tene, the Vice President of Research and Education at the International Association of Privacy Professionals, observed, "[I]t is doubtful . . . that Argentina and Israel, which have both gained adequacy status under the EU Directive, have more robust privacy protection on the ground than the United States or Australia, which have not been certified 'adequate.'"[31]

Concerns with the Directive spurred reform in the EU.[32] The European Parliament and Council agreed on the EU General Data Protection Regulation (GDPR) as the new omnibus data privacy bill in December 2016, which will become effective in May 2018.[33] The difference in form of the GDPR is significant. While the Directive only sets minimum privacy standards, the GDPR, as a regulation, will set the law without need for domestic implementing legislation—a marked centralization of data privacy rulemaking power.[34] The EU touted this change as improved uniformity, which both removes "an obstacle to the pursuit of economic activities" and facilitates the "free flow of personal data."[35]

Substantively, the GDPR retains many features of the Directive, while providing additional protections for EU data subjects. For example, the GDPR maintains the compliance principles outlined in the Directive but adds an "integrity and confidentiality" principle, under which data must be "processed in a manner that ensures appropriate security of the personal data."[36] Notably,

30. This discussion focuses largely on the controversial exclusion of the United States as an inadequate privacy framework. See the treatment of political fears, *infra* Part I.B.2, for a discussion of proposed reforms in Europe to make the data privacy regime even more uniform and controlled by the EU rather than on a country-specific level.

31. Tene, *supra* note 27, at 1232.

32. The European Commission first issued a proposal in January 2012 for revising the Directive. *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 15, 2012), http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF [https://perma.cc/5LFT-LSQ2].

33. GDPR, *supra* note 21.

34. *Id.* art. 1; *see also* BYGRAVE, *supra* note 4, at xxviii; Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1997–2001 (2013).

35. GDPR, *supra* note 21, at 2.

36. *Id.* art. 5.

consent as a basis for data processing remains, largely unchanged.[37] Similarly, the GDPR continues to approve of privately authored binding corporate rules (BCRs) and contract provisions for the transfer of personal data outside the EU.[38] Under the Directive, Germany pushed back on BCRs as a lawful mechanism for data transfer between the United States and Germany.[39] Under the GDPR, however, the difference in form from the Directive is significant. As a "regulation," the GDPR will be effective in member states without implementing member state legislation.[40] This change may herald increased uniformity between member states and decreased confusion for company compliance.

The state of change in EU law raises the question: How does the U.S. privacy framework differ from that of the EU and to what extent do those differences explain the determination that the U.S. framework is not adequate under EU law?

b. U.S. Data Privacy Regulation

U.S. data privacy protection is a subset of the U.S. privacy doctrine, which covers a broad, and occasionally conflicting set of issues.[41] This includes freedom of thought, control over one's body, solitude in one's home, protections from searches and interrogations, protection of reputation, freedom from surveillance, and, most relevant to data privacy, control over personal information.[42] The U.S. data privacy framework includes constitutional, statutory, and executive agency protections, as well as industry self-regulation.[43]

---

37. The GDPR provides that a company may process personal data where it secures "freely given, specific, informed and unambiguous" consent. *Id.* art. 4. The Directive defines consent as "freely given specific and informed." The Directive, *supra* note 22, art. 2.

38. Article 43 of the GDPR formalizes the BCR basic requirements, which were previously identified in a patchwork of Working Papers published by a Directive Article 29 Working Party. *Id.* art. 43.

39. This German Position Paper came in response to the ECJ's determination that the Safe Harbor agreement was invalid under the Directive. Unabhängiges Landeszentrum für Datenschutz (ULD), *ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14* (Oct. 14, 2015), https://www.datenschutzzentrum.de/artikel/981-.html [https://perma.cc/9BR8-MRTQ]. *See also* Michelle Gyves, *German DPAs Announce Policy Severely Limiting Mechanisms for Lawful Germany-to-U.S. Data Transfers*, PROSKAUER (Oct. 26, 2015), http://privacylaw.proskauer.com/2015/10/articles/european-union/german-dpas-announce-policy-severely-limiting-mechanisms-for-lawful-germany-to-u-s-data-transfers [https://perma.cc/KZW2-J6PZ] (raising questions of implementation upon release of the German position paper); *infra* Part I.A.1.c.

40. GDPR, *supra* note 21, art. 1.

41. SCHWARTZ & REIDENBERG, *supra* note 22, at 5–6; *see also* BYGRAVE, *supra* note 4, at 27. Bygrave states that "[v]arious definitions of the concept abound," but there are four principle ways of defining privacy: non-interference; limited accessibility; information control; and protection of intimate or sensitive aspects of one's life. *Id.* Similarly, Daniel Solove has written that the variety of protected areas in privacy creates a problem because courts and privacy practitioners "either conflate distinct privacy problems despite significant differences or fail to recognize a problem entirely." DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 6 (2008).

42. SOLOVE, *supra* note 41, at 6.

43. In addition, U.S. states protect privacy explicitly in state constitutions. *Id.* at 3 n.13.

The starkest difference between the United States and Europe is that the United States does not frame data privacy as a fundamental right. Neither the U.S. Constitution nor the Bill of Rights mentions "privacy." Nonetheless, an interpreted right to privacy has emerged in constitutional jurisprudence.[44] In 1928, Supreme Court Justice Louis Brandeis said privacy was "the most comprehensive of rights and the right most valued by civilized men."[45] This right draws on the First Amendment and the Fifth Amendment protection from self-incrimination, as well as the Fourth Amendment protection against government searches where an individual has a "reasonable expectation of privacy."[46] The Supreme Court bolstered the right to privacy in 1965 by articulating the existence of an individual's protected "zone of privacy," which it subsequently has applied to individuals' decisions about sex, health, and government disclosures.[47] Yet, despite this jurisprudence, the constitutional protection of data privacy is not robust.

These limitations stem from countervailing protections. State action doctrine, for example, generally limits the reach of constitutional rights to private actors, and entanglement does not cover many companies with liability.[48] Much of the current discussion of data privacy in particular deals with private companies' use of data is beyond the reach of constitutional law.[49] In addition, the Fourth Amendment provides little protection of personal information already controlled by a third party or the government.[50] Further, robust privacy regulations face political barriers particularly when weighted against national security and law enforcement, free speech, and economic efficiency.[51] As a

44. One characterization is that "constitutional rights have a positive, if incomplete, effect on data protection law." SCHWARTZ & REIDENBERG, *supra* note 22, at 32.

45. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (holding that wiretapping was not a violation of the Fourth Amendment because the police officers did not enter the home).

46. Katz v. United States, 389 U.S. 347, 360 (1967).

47. Griswold v. Connecticut, 381 U.S. 479 (1965); Eisenstadt v. Baird, 405 U.S. 438 (1972); Lawrence v. Texas, 539 U.S. 558 (2003). Relatively recent Supreme Court jurisprudence, led primarily by Justice Anthony Kennedy, frames privacy in terms of both liberty and dignity. Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 851 (1992) ("These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment."); *Lawrence*, 539 U.S. at 567 ("It suffices for us to acknowledge that adults may choose to enter upon this relationship in the confines of their homes and their own private lives and still retain their dignity as free persons.").

48. *See* Marsh v. Alabama, 326 U.S. 501 (1946).

49. The Snowden revelations have also spurred the debate around data privacy. The 9/11 Commission Report said that government agencies, engaging with greater info sharing with companies, "should 'safeguard the privacy of individuals about whom info is shared,'" and Solove suggested that imprecision in this directive lead to a failure to address it in a meaningful way. SOLOVE, *supra* note 41, at 8.

50. SCHWARTZ & REIDENBERG, *supra* note 22, at 74.

51. SOLOVE, *supra* note 41, at 12.

result, the United States generally regulates data transmission and processing only in specific areas like health and finance, or cases of demonstrable harm.[52]

The most significant U.S. statutory protection of privacy is the Privacy Act of 1974.[53] This statute applies to federal agencies' control of data and requires actual notice, publication, and compatibility of the use with the purpose for which it was collected.[54] It does not operate as an "omnibus bill" that sets a uniform standard like the European Directive, nor does it address the release of information from private industry to the government, although it does regulate private companies' transfer of data to other private actors. The Privacy Act's twelve exceptions further weaken the bill and have been applied in a way to ignore the statutes' limits on data collection and use. The Act requires written release by the information object *unless* the data is intended for a routine use, an exception that critics have called "a huge loophole."[55] In practice, this exception has been used to "justify virtually any disclosure of information without the individual's permission."[56]

Where the Constitution and Privacy Act have not regulated data privacy adequately, executive agencies have performed some gap filling, bolstered further by self-regulation efforts from industries. The Federal Trade Commission (FTC) is the primary enforcement agency for data privacy in the United States.[57] The FTC draws this authority from Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[58] Since 2002, the FTC has brought approximately 100 actions against companies to protect millions of consumers from deceptive and unfair data practices.[59] Under the unfairness prong, the FTC pursues businesses for practices that "cause substantial injury to consumers which is not reasonably avoidable by consumers themselves" and not "outweighed by countervailing benefits to consumers or to competition."[60] Under the deception prong, the FTC targets those practices that violate the business' own stated policies.

The breadth of the FTC Act has enabled the agency to adapt to changing technologies and practices. Some have lauded the emergence of FTC "common law of consent decrees" as providing flexible rules for companies' data privacy

52. Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25, 31 (2013).

53. Privacy Act of 1974, 5 U.S.C. § 552a (2012).

54. SCHWARTZ & REIDENBERG, *supra* note 22, at 92, 96.

55. DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 323 (1989) (comparing data privacy in the United States and Europe).

56. SCHWARTZ & REIDENBERG, *supra* note 22, at 95.

57. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 248 (3d Cir. 2015). The Department of Commerce, the Federal Reserve Board, and the Office of Management and Budget also have important roles that are not under the purview of this Note.

58. Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2012).

59. BRILL, *supra* note 1, at 3.

60. 15 U.S.C. § 45(n).

compliance.[61] The FTC is limited, however, to protecting consumers, and, even in regards to consumers, the FTC authority does not extend to financial institutions (regulated by the Federal Reserve Board), common carriers (regulated by the Federal Communications Commission), insurance companies, and nonprofit organizations.[62] Moreover, although the FTC can enforce company promises and trade-wide self-regulation, it has less authority where the company did not breach consumer expectations.[63] The FTC is to some extent empowered by self-regulating agreements and privacy statements because they set consumer expectations, but such self-regulation statements also set a cliff.[64]

Overall, commentators have found that the U.S. framework protects data privacy fairly well, although not in a way that closely resembles the European system.[65] These proponents say that those who repeat the "notion" that the United States does not have a privacy framework "do not fully understand" the U.S. system.[66] Points of shared values indicate the potential for agreement beyond differences.

c. U.S.-EU Data Agreements

Despite the European assertion that the U.S. system is not adequate, the economic demand for transborder data flow has pressured both sides to find a way to allow this exchange. In 2000, the United States and EU entered into the Safe Harbor agreement.[67] Under Safe Harbor, the U.S. Department of Commerce granted year-long certification to U.S. companies that satisfied the Safe Harbor agreement's seven privacy principles, such as notice, choice, access, and

---

61. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1227 n.46 (citing Christopher Wolf, Targeted Enforcement and Shared Lawmaking Authority as Catalysts for Data Protection 2 (presented at 32nd Annual International Conference of Privacy and Data Protection Commissioners, Oct. 27–29, 2010)); *see also* Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority as Catalysts for Data Protection*, BNA PRIVACY & SECURITY L. REP. (Oct. 25, 2010), http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WolfDataProtectionandPrivacyCommissioners.pdf.

62. 15 U.S.C. § 45(a)(2).

63. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1237. Tene discusses the Sears case, in which the FTC found Sears had misled consumers by failing to disclose the scope of personal information its software would monitor. *Id.* Tene notes that if Sears had been more forthright about its practices, the FTC would have had fewer enforcement options. *Id.*

64. *But see* Complaint ¶ 14, *In re* DesignerWare, LLC, Docket No. C-4390 (F.T.C. Apr. 11, 2013), http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf [https://perma.cc/T566-NQNT] (the FTC brought an action against a company that, without the customers' knowledge, used software to log customers' key strokes on rent-to-own computers and to take pictures with the computers' webcams).

65. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529, 1548–49 (2013); BRILL, *supra* note 1, at 2; Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1226–27 (comparing reform efforts and shortfalls in the EU and United States).

66. BRILL, *supra* note 1, at 2.

67. *Safe Harbor Privacy Principles*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018475.asp [https://perma.cc/9TPE-XUYF] (last updated Jan. 30, 2009); Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC).

enforcement.[68] Once certified, a company was deemed to provide adequate privacy protection to all individuals in member states of the EU.[69] The Safe Harbor agreement grew to include more than 4,000 companies across forty sectors, an indication of the extent to which the transatlantic economy relies on international data transfers and is willing to follow established, shared guidelines.[70]

In October 2015, the European Court of Justice (ECJ) declared the Safe Harbor agreement "invalid," citing concerns with the level of privacy protection it provided and recent "revelations made by Edward Snowden."[71] The U.S. Commerce Department and the European Commission anticipated and responded to this determination by developing the U.S.-EU Privacy Shield Framework, which replaced Safe Harbor and went into effect on July 16, 2016.[72] The ability of the United States and EU to adapt to the ECJ ruling in a relatively short period reflects their shared political and economic interests in maintaining and improving transatlantic data flows.

The Privacy Shield has many similarities to the Safe Harbor approach, and some new features. For example, the Privacy Shield maintains the Safe Harbor's seven guiding principles and also adds on sixteen "supplemental principles."[73] U.S. companies still self-certify with the Department of Commerce, and they are required to publicly declare their compliance so that their commitment is enforceable under U.S. law.[74] In addition, the Privacy Shield further limits U.S. government access to data, creates direct and cost-free redress avenues for individuals, and institutionalizes an annual joint review.[75]

---

68. EXPORT.GOV, *supra* note 67.

69. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp [https://perma.cc/7JKH-7JSA] (last updated Dec. 18, 2013).

70. *See* JULES POLONETSKY ET AL., FUTURE OF PRIVACY FORUM, THE US-EU SAFE HARBOR: AN ANALYSIS OF THE FRAMEWORK'S EFFECTIVENESS IN PROTECTING PERSONAL PRIVACY, at ii (2013), http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf [https://perma.cc/L5X6-X4RB].

71. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-1, ¶¶ 28, 30, 98.

72. Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1 (EU).

73. U.S. DEP'T OF COMMERCE, EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES (2000), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [https://perma.cc/37C5-ZYF5]. The sixteen supplemental principles are: sensitive data, journalistic exceptions, secondary liability, performing due diligence and conducting audits, the role of the data protection authorities, self-certification, verification, access, human resources data, obligatory contracts for onward transfers, dispute resolution and enforcement, choice—timing of opt out, travel information, pharmaceutical and medical products, public record and publicly available information, access requests by public authorities. *Id.*

74. U.S. DEP'T OF COMMERCE, FACT SHEET: OVERVIEW OF THE EU-U.S. PRIVACY SHIELD FRAMEWORK 1, 4 (2016), https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework [https://perma.cc/JL4G-TPPB]; EUROPEAN COMM'N, EU-U.S. PRIVACY SHIELD (2016), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf [https://perma.cc/V8U3-RH83].

75. *See* U.S. DEP'T OF COMMERCE, *supra* note 74; EUROPEAN COMM'N, *supra* note 74.

2. Non-binding

In addition to the binding instruments for data privacy, there are also non-binding declarations, guidelines, and frameworks that guide privacy in transborder data flow. The 1948 Universal Declaration of Human Rights (UDHR)[76] was the first document to set out universal human rights norms, and it recognized a right to privacy.[77] Interestingly, although the characterization of privacy as a fundamental right defines the European approach, an initial draft of the UDHR more closely mirrored the Fourth Amendment of the U.S. Constitution, which draft read, "No one shall be subjected to arbitrary searches or seizures, or to unreasonable interference with his person, home, family relations, reputation, *privacy*, activities, or personal property."[78] This *travaux préparatoires* reinforces the theory that although the two frameworks find themselves at loggerheads over what constitutes adequate privacy protection, they started from shared principles.

Following the UDHR and midcentury privacy movement, articulations of multilateral privacy standards have emerged from economic international organizations rather than from the United Nations. In 1980, the Organization for Economic Co-operation and Development (OECD)[79] created non-binding Privacy Guidelines.[80] The original OECD transborder data flow provision was based on an "adequacy" rationale, which is similar to, but more loosely stated than, the standards included in the European Directive.[81] Multinational privacy guidelines indicate points of shared interests and norms and have exercised localized influence in domestic law.[82]

In addition, contemporary multilateral data privacy agreements have included trade-based, rather than rights-based, language. For example, the Asia Pacific Economic Cooperation (APEC) agreed to a Privacy Framework in

76. G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

77. *Id.* Article 12 reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.* art 12.

78. Diggelmann & Cleis, *supra* note 14, at 441, 445.

79. Member states include Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland; France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States. *Members and Partners*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/about/membersandpartners [https://perma.cc/5UQJ-XMPM].

80. ORG. FOR ECON. CO-OPERATION & DEV., RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/TBP9-VK57].

81. *See* Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1231; *supra* Part I.A.1.a (discussion of the EU Directive).

82. BYGRAVE, *supra* note 4, at xxv. Privacy rights are enshrined in constitutions around the world "[i]n nearly every nation." SOLOVE, *supra* note 41, at 2.

2004.[83] Economic concerns are predominant, such as preventing "commercially harmful restrictions on transborder data flow."[84] This measure seemingly fosters data privacy less because of a naturalist desire to protect human rights, and more from the self-interested goal of building consumer confidence.[85] The United States, an APEC member, has used consumer confidence as a model in data privacy regulation to some success.[86] Also, the APEC Framework does not stray significantly from the OECD Guidelines. It includes information privacy principles (IPPs) such as "notice" and "choice," reflecting the influence of the Safe Harbor Agreement beyond transborder data flow between the United States and European Union.[87]

Finally, recent reform in the OECD Guidelines reflects an accommodation of increasingly non-geographic location of data. The OECD Recommendation introduced revisions in 2013 that included a shift to an accountability model, which holds organizations responsible for personal data under their control without regard to location, marking a shift to decreased emphasis on geographic restrictions on transborder data flows.[88] This accountability model serves as a useful example for reform of U.S.-EU privacy regulations.

B. Values

Shared values and statements about data privacy are valuable common ground in negotiations for an agreement between the United States and Europe. Such points of international agreement, particularly shared norms and concerns between the United States and Europe, can be useful in bridging the differences between their existing digital privacy frameworks. However, distrust and fear of the others' approach have created an environment hostile to reconciliation of the two regimes.

---

83. APEC members include Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, the Russian Federation, Singapore, Taiwan, Thailand, the United States, and Vietnam. *Member Economies*, ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx [https://perma.cc/U7RV-LK4R].

84. BYGRAVE, *supra* note 4, at 75–76.

85. *Id.* at 75. The APEC Framework states the OECD Guidelines "[i]n many ways . . . represent the international consensus on what constitutes honest and trustworthy treatment of personal information." ASIA-PACIFIC ECON. COOPERATION, APEC PRIVACY FRAMEWORK 3 n.1 (2005), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx [https://perma.cc/6D64-7NA3].

86. Bamberger & Mulligan, *supra* note 65, at 1555, 1561 (discussing the increase in U.S. privacy requirements that reflect a growing focus on consumer expectations).

87. BYGRAVE, *supra* note 4, at 76.

88. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1232; ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 11–17 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/7YBS-99ER].

1. Substantial Points of Commonality

Differences between the United States and Europe regarding adequate data transfer and processing safeguards are significant, but not irreconcilable. There are indications of common ground in four areas, suggesting that some unified standard of data privacy that would allow freer data transfers is within reach.

First, and fundamentally, both the United States and the EU agree that the prevention of harm to data privacy is an important concern and that the free flow of data is a common good. Both acknowledge a right to privacy in international and domestic law, which informs domestic data privacy frameworks.[89] Then-FTC Commissioner Julie Brill expressed optimism about resolving tensions with Europe, saying she was confident because of the "common privacy principles that we share, and the efforts underway on both sides of the Atlantic to examine whether our different privacy frameworks are able to sufficiently protect consumers in an era of big data and the Internet of Things."[90] These commonalities are starker when compared to other countries. There are indications that China's valuation of privacy is so different from the U.S. or EU model that the latter two may be spurred towards greater coordination and convergence.[91] Some academics and practitioners similarly debate whether the two regulatory frameworks are even so divergent. Professors Kenneth Bamberger and Deirdre Mulligan have argued that numerous factors in the U.S. system enable greater privacy protection than the rules alone indicate.[92] Omer Tene has compared the EU Directive's clause permitting data use without consent where it is in the "legitimate interests of the controller" to the U.S. "unfair practices" standard.[93] Both approaches enable the consideration of multiple benefits and avoid some of the pitfalls of a consent-based approach.[94] Even voices that contrast the approaches to privacy in the United States and Europe, such as James Whitman, start from the premise that both frameworks value privacy "as a supremely important human good."[95]

89. *See* discussion, *supra* Part II.

90. BRILL, *supra* note 1, at 11.

91. Tourkochoriti, *supra* note 2, at 175–76.

92. For instance, Bamberger and Mulligan described ways in which the German and U.S. approaches are both similar frameworks, and similarly effective. Bamberger & Mulligan, *supra* note 65, at 1571.

93. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1248; *see also* Polonetsky & Tene, *supra* note 52. Article 7 of the EU Directive permits data processing absent individual consent, based on the legitimate interests of the company controlling the data as balanced against the individual's privacy rights. *See* The Directive, *supra* note 22, art. 7(f) ("[P]rocessing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article1(1).").

94. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1227. He concludes, however, that the standard is applied inconsistently in various jurisdictions, and the lack of certainty leads organizations to revert to individual consent. *Id.*

95. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1153 (2004). Whitman suggests that different cultural sensibilities manifest in "social

Second, the U.S. and European frameworks share some problems that have arisen from developments in technology and experience. For example, the reliance on consent poses a threat to individual data privacy in either existing framework. Consent to data use is widely regarded as "seldom meaningful, voluntary, and fully informed."[96] Consent puts too much pressure on individuals to track the use of their data in a way they should not be expected to do. The data's uses are complex and inscrutable, and moreover, consumers have little bargaining power to change the use provisions that they are asked to accept.[97] These problems have given rise to reform, which is ongoing in both the United States and Europe. A shared, reformed model would put less of a burden on individuals in balancing fundamental protection and freeing up the process.

Privacy concerns among individuals in the United States and Europe are also similar: surveys show levels of concern are relatively high, reflecting pessimism about existing levels of privacy and distrust that organizations may misuse personal information.[98] Although both the United States and Europe are dominant actors in data privacy regulation, neither currently has an ideal domestic framework that justifies adoption by the other.

Finally, the robust economic links between the United States and the EU and the growing market for data has put pressure on these two systems to come together. The European Commission explains the rationale for its regional approach to data privacy regulation on its website with this statement: "[e]very day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges."[99] The Commission goes on to say, "[t]he individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries."[100] This economic reasoning applies to transatlantic flow of data as well. Economists agree that barriers to trade are harmful overall because they impede competition in a free market. Shifting to consider data flow as a trade issue would bring this powerful market consideration into account and help both the United States and the EU to maximize the social utility of the data trade.

---

misunderstanding[s]" or may erupt into greater "legal and trade battles," such as the ongoing discussion around the divergent approaches to protecting consumer data. *Id.* at 1156.

96. *Id.* at 1245; *see also* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341, 364 (Jane K. Winn ed., 2006) ("Notice and consent requirements often create the illusion, but not the reality, of meaningful consumer choice.").

97. *See* Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1245.

98. BYGRAVE, *supra* note 4, at 21–23. Nonetheless, there is also an indication also that individuals are increasingly acclimatized to the divulgence of their personal information. In particular, "digital natives," those born after 1980 who are comfortable handling most transactions online, are less concerned about data privacy than older generations. *Id.* at 22–23.

99. *Protection of Personal Data*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection [https://perma.cc/9JK8-LURL].

100. *Id.*

2. Distrust and Fear Are Roadblocks to Interoperability

Despite the foundation of international and regional agreements and shared values on data privacy, the differences in the two frameworks have fostered a level of distrust that has proven politically difficult to overcome. Revelations of U.S. surveillance energized European legislators to enhance its rules and scrutinize U.S. practices.[101] The current reform of European regulations reflects this politically difficult climate; the development of the Privacy Shield and GDPR had the personal data use of both the U.S. government and U.S. companies in mind.[102] These revisions may lead to a greater "collision" with the U.S. data privacy regulations, elevating some rights beyond U.S. law.[103] At the least, these provisions indicate the extent to which Europe has focused on enhancing the Directive or the Safe Harbor Agreement, despite similar values with the United States and the borderless nature of data in the cloud.

Nonetheless, the U.S. government and private companies have lobbied the EU for greater acceptance of U.S. practices. These efforts have included both a greater acceptance of U.S. practices as adequate for EU regulations and efforts to reform EU rules to align more closely with the U.S. model. For example, then-U.S. Department of Commerce Assistant Secretary Lawrence Strickling stated that discussions about privacy regulation between U.S. and European governments were primarily to achieve "interoperability" between the two systems.[104] Interoperability is about finding a way for different privacy frameworks to work together without necessarily changing the way U.S. corporations do business.[105] Pressure from the Obama administration successfully led to the deletion of some text from the draft GDPR before it was first published.[106]

U.S.-based companies have added their lobbying efforts to those of the government. Google, Yahoo, Facebook, Amazon, and eBay have each spent millions of dollars in lobbying against the EU privacy regulations that limit the processing of an Internet user's personal information.[107] These companies targeted the draft GDPR provisions that would require member states to let users opt out of targeted advertising (a measure similar to the "Do Not Track" bill promoted by West Virginia Sen. Jay Rockefeller in the U.S. Congress), as well

101. BYGRAVE, *supra* note 4, at xxviii.

102. *See, e.g.*, Sam Schechner, *France Wants EU Data Privacy Rules to 'Balance' U.S. Web Giants' Power*, WALL STREET J. (Dec. 8, 2014), http://blogs.wsj.com/digits/2014/12/08/france-wants-eu-data-privacy-rules-to-balance-u-s-web-giants-power [https://perma.cc/QVA4-9CP5] (noting that French Prime Minister Manuel Valls announced support for stricter data privacy regulations to "maintain a balance of power").

103. Schwartz, *The EU-U.S. Privacy Collision*, *supra* note 34, at 1994–97.

104. Dana Liebelson, *Ex-White House Official Joins Group Fighting "Excessive" Online Privacy Laws*, MOTHER JONES (Mar. 29, 2013), http://www.motherjones.com/politics/2013/03/daniel-weitzner-internet-privacy-coalition [https://perma.cc/5QXD-C6AJ].

105. *Id.*

106. *Id.*

107. *Id.*

as establish the right for users to erase personal information from indexes like Facebook or Google searches.[108]

However, this push for interoperability has faced criticism both in the United States and across Europe. The Director of the American Civil Liberties Union's Speech, Privacy, and Technology Project, Ben Wizner, said this focus could lead to a scenario where "interoperability becomes this race to the bottom, where the weaker protections of the American system are exported to Europe and the world."[109] Wizner also critiqued certain European regulations such as the right to be forgotten as too constricting on free speech.[110]

There is a need and a space for both sides to come to consensus. Success should be measured by agreements that promote data privacy and trade—not the dominance of one domestic privacy framework over another.

II.
DATA PRIVACY AS TRADE

Differences between U.S. and European approaches to data privacy rules and enforcement indicate the need for a legal framework that better unifies the two systems. This Part proposes that the repositioning of data privacy into a trade framework could better take into account the growing market for transborder data flow. This shift has the potential to enable the beneficial flow of data, while protecting privacy and other countervailing interests. Part II.A introduces the characteristics of a "trade framework," particularly the potential to enable value exchanges between independent states, using measures designed to facilitate competition and, on occasion, raise protection standards. To explain the proposed application of the trade framework to data privacy, the Section identifies prior instances when an emerging global market was incorporated into a trade framework. Part II.B then describes the growing, influential, and global market for data.

A. Trade Framework Characteristics

The global trade framework seeks to enable the exchange of goods and services between sovereign states that are inherently different. Traditional trade theory views states according to their comparative advantages, resource endowments, regulatory standards, and organization as a market- or nonmarket-based economy. David Ricardo developed the theory of pure trade and comparative advantage, which states that where the relative prices of goods differ between countries, some will gain and none will lose if the good were

108. *Id.*
109. *Id.*
110. *Id.*

offered at an intermediate world price without tariffs or other barriers to trade.[111] This theory assumes perfect competition, in which global supply and demand would lead to a more efficient allocation of resources and production, bestowing a benefit on all actors.

Fundamentally, the framework of international trade, which bridges (and even capitalizes on) differences between countries allows for the imposition of some shared regulatory constraints. Although the rhetoric of global trade emphasizes "free trade," or the removal of tariff and nontariff barriers, in practice, international trade law is defined just as much by the constraints it imposes. For example, over 50 percent of world trade occurs within regional trade areas, such as the North American Free Trade Area (NAFTA), and negotiated customs unions, such as the EU. These free trade areas allow for the removal of tariffs among member states so long as tariff levels with states outside of the area do not increase. This arrangement is an exception to the "most favored nation" principle under which all imports should be given equal treatment, regardless of the country of origin. This suggests that trade is not only a tool of tariff deregulation but also a potential regulatory instrument.

International trade law also permits some protective domestic regulation that it would otherwise prohibit as discriminatory. For example, Article XX(g) of the General Agreement on Tariffs and Trade (GATT) allows an exception for domestic measures that conserve exhaustible natural resources.[112] This exception made permissible flexible shrimp fishing regulations in the United States to protect sea turtles better.[113] This again is an example of the framework allowing for constraints, in this case to reach shared policy goals.

Furthermore, the trade law framework enables countries to agree on uniform regulatory standards that also protect the level playing field for competition. Such agreements can occur at the World Trade Organization (WTO),[114] binding all 161 WTO member states, or bilaterally between just two states.

Significantly, the WTO has incorporated an area of the global market into a trade framework before, as it did with the General Agreement on Trade in

111. *See generally* DAVID RICARDO, THE PRINCIPLES OF POLITICAL ECONOMY AND TAXATION (Chris Cowlin ed., Empiricus Books 2002) (1817); ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (Edwin Cannan ed., Methuen & Co., Ltd. 1904) (1776).

112. General Agreement on Tariffs and Trade 1994 art XX(g), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, Legal Instruments—Results of the Uruguay Round vol. 1 (1994), 1867 U.N.T.S. 187, 33 I.L.M. 1153 [hereinafter GATT 1994].

113. Panel Report, *United States—Standards for Reformulated and Conventional Gasoline (Treatment of Imported Gasoline and Like Products of National Origin)*, WTO Doc. WT/DS2/R, 35 I.L.M. 274 (1996).

114. *Members and Observers*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm [https://perma.cc/CD9J-FD2C]. For example, the Sanitary and Phytosanitary Agreement (SPS) sets standards for plant and human health.

Services (GATS).[115] The GATS was a product of the internationally negotiated 1994 Uruguay Rounds, which also created the WTO Charter, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and an updated version of the GATT.[116] The GATS borrowed from the established nondiscrimination principles, which governed the trade in goods under the GATT, and applied them to service fields such as finance, education, tourism, communication, and licensing.[117] Proponents for reframing services in the trade framework argued that services composed a significant and growing portion of international trade in foreign markets, and that a failure to provide protection posed a barrier to trade.[118] Europe and the United States, the primary exporters of services, were particularly strong advocates for the GATS.[119] The agreement allowed them to secure a level of protection from foreign domestic regulations that were not as robust as their domestic rules.[120] This is a significant benefit that may be achieved again with an incorporation of the transborder data flow market under a WTO standard.

In addition to WTO binding agreements, uniform trade standards may develop regionally through multilateral or bilateral trade agreements. Some observers advocated for the inclusion of similar data transfer provisions in the Trans-Pacific Partnership (TPP), the proposed regional trade agreement between the United States and several Asian countries.[121] The Transatlantic Trade and Investment Partnership (TTIP), a proposed trade agreement between the United States and Europe, presents an opportunity to set broadly applicable standards at a regional level. This type of regional trade agreement between the United States

115. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, Legal Instruments—Results of the Uruguay Round vols. 28–30 (1994), 1869 U.N.T.S. 183, 33 I.L.M. 1168 [hereinafter GATS].

116. General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194. The GATT was reaffirmed in 1994, as the GATS was created. *See* GATT 1994, *supra* note 112; GATS, *supra* note 115.

117. GATS art. 1 ("'[S]ervices' includes any service in any sector except services supplied in the exercise of governmental authority."); *see also* WORLD TRADE ORGANIZATION, TRADE IN SERVICES 3 (2015), https://www.wto.org/english/thewto_e/20y_e/services_brochure2015_e.pdf [https://perma.cc/AEE3-9EYP].

118. Juan A. Marchetti & Petros C. Mavroidis, *The Genesis of the GATS (General Agreement on Trade in Services)*, 22 EUR. J. INT'L L. 689, 692–93 (2011).

119. *Id.* at 692–95.

120. *Id.* at 690–92; *see also* Caroline Dommen, *Migrants' Human Rights: Could GATS Help?*, MIGRATION POLICY INST. (Mar. 1, 2005), http://www.migrationpolicy.org/article/migrants-human-rights-could-gats-help [https://perma.cc/Y6RK-JTZB] (explaining that most countries that made early commitments to GATS provided for "wage and labor standard parity").

121. MacDonald & Streatfeild, *supra* note 6, at 630–31 (considering the implications of the trade agreement). Evolving politics in the United States have rendered the nearly completed TPP now seemingly impossible to complete. *See, e.g.*, Isabel Reynolds & Michael Heath, *Australia Pushes for TPP Without U.S. After Trump Exits Deal*, BLOOMBERG (Jan. 23, 2017), https://www.bloomberg.com/news/articles/2017-01-24/australia-leads-push-for-tpp-without-u-s-after-trump-exits-deal [https://perma.cc/9RZ2-ZZUQ].

and the EU could include transborder data flow as a trade issue, while also setting and protecting shared privacy standards.

Recent trends in U.S. politics suggest regional agreements such as the TPP or TTIP may be less palatable than bilateral trade agreements. The U.S. government hailed the U.S.-Korea Free Trade Agreement (KORUS FTA) as a "groundbreaking" bilateral agreement, particularly for its provision for data transfers in financial services, as well as its protections for workers' rights and the environment.[122] These country-to-country agreements may provide for greater ease in negotiation, enabling the achievement of an agreement like KORUS FTA, but they also reduce the potential breadth of shared rules across national borders that a WTO or regional agreement would afford.

In this context, it is possible that competing interests between valuable data flow and privacy have put data privacy "on a collision course with international trade rules now more than it ever has in the past."[123] But, given the characteristics of the trade framework, a more optimistic outcome seems plausible: the existing trade framework could fluidly absorb data flow and define uniform standards that both offer enhanced protection and facilitate the utilities of exchange.

B. The Global Data Market

Like the rise of the trade in services that preceded the creation of the GATS, the foremost reason to frame data privacy as trade is that data flow has become a huge global industry. This is apparent both in terms of the value of the product and the transnational character of the trade. Commentators have termed personal data "the new 'oil,'" a reflection of its market surge over the past twenty years.[124]

Data has many uses. Companies buy data and sell the analysis, which enables businesses to engage in targeted marketing and credit risk analysis. Data itself can also be used for a variety of purposes: improved diversity recruitment in the workplace, identification of disparities in services, and monitoring and improving access to health and human services.[125] Medical research has

122. United States-Korea Free Trade Agreement, U.S.-S. Kor., June 30, 2007, 125 Stat. 428, 46 I.L.M 642; Press Release, The White House, Office of the Press Sec'y, Remarks by the President at the Announcement of a U.S.-Korea Free Trade Agreement (Dec. 4, 2010), https://obamawhitehouse.archives.gov/the-press-office/2010/12/04/remarks-president-announcement-a-us-korea-free-trade-agreement [https://perma.cc/2FKV-UK4U]; *see also* MacDonald and Streatfeild, *supra* note 6, at 626.

123. MacDonald and Streatfeild, *supra* note 6, at 626. The authors suggested that cross border service disputes and data privacy issues are therefore international trade's new frontier. *Id.* at 633.

124. WORLD ECON. FORUM, PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS 5 (2011), http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf [https://perma.cc/NP4J-T5BA].

125. *See* KUNER, *supra* note 5, at 5. Global Pulse is a UN organization that conducts research and partners with countries and the private sector to protect vulnerable populations better, including initiatives like the Health Map project, which tracks the spread of infection disease. U.N. GLOBAL PULSE, BIG DATA FOR DEVELOPMENT: CHALLENGES & OPPORTUNITIES 4 (2012), http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf [https://perma.cc/LR3C-LDX2]; *see also* JAMES MANYIKA ET AL.,

benefited through the use of big data to improve the understanding of fatal diseases as well as patterns between drugs and negative side effects. Similarly, social policy and responsiveness have been enhanced in urban planning and disaster relief with the help of big data.[126] Data has increasingly been used in the public sector for national security protection and law enforcement as well.[127] The benefits are significant, cross industries, and have become expected to some extent in the delivery of goods and services.

In addition, personal data has become a type of currency, given by individual users online for otherwise "free" Internet services and programs like those that Google and Facebook provide.[128] A consumer, eager to have access to the content or app, typically thinks of giving personal data as a byproduct of the transaction, whereas a vendor seeks the information as part of the primary value proposition of the offered service. This is part of a broader shift, in which individuals have a greater role in the transmission of their data than ever before. The cost of transferring data over computer networks was high in the 1970s when some of the major regulations were established. Today, the cost of Internet access is not a barrier to individuals engaging in transborder data transfers.[129] Communications, social networking sites, and mobile apps have become widely used, and individuals choose to put personal information on the Internet through a variety of instruments such as location identifiers, reviews of goods and services, and peer produced content that provides detailed information about their family and friends.[130] The rise of the Internet of Things also relies on

---

MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY (2011), http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_Data_The_Next_Frontier_for_innovation [https://perma.cc/S8R3-RFKL] (predicting that analyzing big data will become a fundamental basis of competition); Omer Tene & Jules Polenetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 246 (2013) (discussing the discovery by Kaiser Permanente of a connection between the drug Vioxx and cardiac arrests through clinical and cost data); Christopher Wolf, *The Commercial Use of Big Data Can Help Improve Equality*, N.Y. TIMES (Aug. 7, 2014), http://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/the-commercial-use-of-big-data-can-help-improve-equality [https://perma.cc/CH7A-N92S].

126. Polonetsky & Tene, *supra* note 52, at 30. Polonetsky and Tene have identified benefits to individuals, community, organizations, and society. *Id.* at 28–30. These range from small conveniences, such as Google autocomplete and Netflix and Amazon customization at the individual level, to business efficiency at the organization level, to national security, energy efficiency, and disaster response at the society level. *Id.*

127. Polonetsky and Tene argue that benefits should be incorporated in privacy assessments along with risks. *Id.* at 30. Separately, Tene proposed that consent may be an improper requirement where anticipated benefits to society are compelling and risks to individuals are small. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1247.

128. *See* KUNER, *supra* note 5, at 6 (citing Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability*, 00062/10/EN WP 173 (July 13, 2010), at 5); MacDonald & Streatfeild, *supra* note 6, at 626 ("Personal data has been labeled the 'currency' of the digital economy.").

129. KUNER, *supra* note 5, at 6.

130. *Id.* at 4; Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1229.

individuals' decisions to transmit personal data, potentially raising unknown risks of improper access or abuse of the data.

The transborder data market also reflects the changing economic landscape brought about by globalization and trade liberalization.[131] Globalization has accelerated with advancements in technology, communications, and industry—all of which decrease the utility of divergent, country-specific regulatory standards in commerce and trade.[132] In the past, data transfers were typically transmitted from one discrete point to another. Today, transfers of data are "ubiquitous, geographically indeterminate, and typically 'residing' in the cloud."[133] Geography and jurisdiction remain "key factors for the application of data protection and privacy law," but, in the market for transborder data flow, "[m]any companies structure their operations based on lines of business rather than geography, and technology allows the transfer of personal data without regard to national borders."[134] With cloud-based storage, processing, and transmission, the location of the data "becomes indeterminate, indeed unimportant,"[135] and, in turn, national borders have less significance than before.

In terms of demand, utility, and operations, transborder data flow has become a major global market that would benefit from a more international form of regulation.

III.
APPLIED: U.S.-EU DATA TRANSFERS AS TRADE

A substantial part of the global trade in data occurs between the United States and the EU. The economic relationship between the United States and the EU is the largest in the world, and the two regions account for 30 percent of world trade.[136] Electronic commerce represents 10 percent of growth in GDP in the world's most developed economies in the last fifteen years, and, according to estimates from the European Commission, over half of the U.S.-EU cross border trade in services depends on the Internet.[137] Remarkably, despite the controversial and shifting legal context of the Safe Harbor agreement and Privacy Shield, the two regions have the highest rate of cross border data exchange in the world.[138] In 2013, the United States and the EU began

131. *See* KUNER, *supra* note 5, at 2.

132. *Id.*

133. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1218. Cloud computing includes (i) software as a service provided by a business to a consumer, such as e-mail, instant messaging, and photosharing tools, as well as business-to-business services like customer relationship management; (ii) platform services; and (iii) infrastructure as a service, such as facilities for storage, computing, and networking. *Id.* at 1229.

134. KUNER, *supra* note 5, at 3.

135. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1229.

136. Tourkochoriti, *supra* note 2, at 161.

137. *Id.* at 162.

138. Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for the U.S. and EU Trade and Investment* 1 (Brookings Inst., Global Econ. & Dev., Working Paper No. 79, 2014),

negotiations for the Transatlantic Trade and Investment Partnership (TTIP), a free trade agreement intended to eliminate further barriers to trade.[139] If the agreement is reached, it would be unprecedented in its scale due to the size of the trade between the two regions.[140]

Part III.A introduces the initiative that data privacy be a feature of the negotiated trade agreement between the United States and the EU. Part III.B then offers an alternative approach, applying the trade framework Part II outlined to the U.S.-EU economic relationship and identifying three significant benefits.

A. Proposed Inclusion of Data in a U.S.-EU Trade Agreement

Some U.S. organizations have pushed to include measures for "digital free trade" and interoperability in the TTIP. Vocal advocates include the Coalition for Privacy and Free Trade, an organization open to all companies that collect, use, and transfer personal data,[141] and the Free Privacy Forum (FPF), which promotes industry-led self-regulation for data privacy.[142] The FPF has focused its lobbying efforts on the U.S. International Trade Commission Investigation on Digital Trade[143] and the TTIP.[144] According to Christopher Wolf, who helped mobilize both the Coalition for Privacy and Free Trade and the FPF, these initiatives seek to encourage the U.S. government to convince the EU to recognize U.S. privacy regulations as "'adequate,' thus allowing the free flow of

---

https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf [https://perma.cc/FTF9-WELJ].

139. *The Transatlantic Trade Investment Partnership*, EUROPEAN COMM'N, http://ec.europa.eu/trade/policy/in-focus/ttip [https://perma.cc/QR2F-A9RW] (last updated Feb. 9, 2017). Meanwhile, Canada finalized its trade agreement with the EU, pending consent of the European Parliament. Comprehensive and Economic Trade Agreement (CETA), Can.-EU (unratified as of July 1, 2017), http://data.consilium.europa.eu/doc/document/ST-10973-2016-INIT/en/pdf [https://perma.cc/9N73-UMN6].

140. Ioanna Tourkochoriti, *The Snowden Revelations, The Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU in Data Privacy Protection*, 36 UALR L. REV. 161, 161 & n.2 (2014).

141. Liebelson, *supra* note 104.

142. The FPF created a smart grid privacy seal program using input from industry and utility regulators and intended for use by companies that provide consumer services that rely on energy data. Christopher Wolf, *Law of the Connected Horse? FTC Appropriately in Learning Mode on Internet of Things*, INT'L ASS'N OF PRIVACY PROF'LS (Nov. 14, 2013), https://privacyassociation.org/news/a/law-of-the-connected-horse-ftc-appropriately-in-learning-mode-on-internet-o [https://perma.cc/4NHG-XVZ7]. FPF also worked with Senator Charles Schumer (D-NY) and a group of "location analytics companies to release a Code of Conduct designed to promote consumer privacy and responsible data use in association with retail location analytics." *About Smart Places*, FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/issues/smart-places [https://perma.cc/6WLU-EGS4].

143. The U.S. Trade Commission defines "digital trade" as commerce in products and services delivered over digital networks, including software, digital media files (such as e-books and digital audio files) and services such as data processing and hosting. Digital Trade in the U.S. and Global Economies, Part I; Institution of Investigation and Scheduling of Hearing, 78 Fed. Reg. 2690 (Jan. 14, 2013).

144. *See* Christopher Wolf, *Trade Law and Privacy Law Come Together*, INT'L ASS'N OF PRIVACY PROF'LS (Feb. 21, 2013), https://privacyassociation.org/news/a/trade-law-and-privacy-law-come-together [https://perma.cc/8K6C-R2M8].

data across borders."[145] More generally, it would create a blueprint for "how to harmonize the distinct approaches to privacy protection on the respective sides of the Atlantic so that multi-national businesses can operate smoothly in all jurisdictions."[146]

This unusual proposal faces strong opposition, particularly from European officials. The EU, wary of U.S. privacy regulations, generally wants to exclude "digital free trade" from the TTIP. Franz Obermayr, an Austrian member of the European Parliament articulated generally held EU concerns with the U.S. Trade Commission:

> [T]he European and American approaches could hardly be more different, whether regarding access to bank data or to data in 'clouds'. . . . Given that the use of the Internet plays a key role in an increasing number of areas of daily life, and that frequently several undertakings are involved in providing a given service, in a transatlantic internal market, it would become even harder to guarantee European data protection standards.[147]

This reluctance among EU officials to accept U.S. practices as "adequate" is a significant barrier for any initiative to approach data as a trade issue, and ultimately will frustrate the efforts of the Coalition for Privacy and Free Trade and the FPF. Europe wants greater guarantees of existing privacy protections and distrusts U.S. businesses to self-regulate.[148] The following Section discusses an alternative to an adequacy approach and identifies three anticipated benefits.

B. A Regional, Consumer-Based Alternative

Agreement on the adequacy of U.S. privacy regulations is not the only possible approach to data as trade. As discussed in Part II, international trade law accommodates varying domestic regulatory regimes that provide protection for individuals and businesses. The WTO facilitates universal standards, but does not dictate the content of domestic regulation. This is also the case with the outgoing EU Directive, which establishes regional standards but leaves the content of domestic privacy policies to individual states.

The existing common ground between the U.S. and EU privacy frameworks, discussed in Part I, could serve as the foundation for an agreement on permissible data trade practices. As discussed in Part II, this agreement could

---

145. *Id.*

146. *Id.*

147. *Id.*

148. For example, the French National Commission on Informatics and Liberty and an EU data protection advocacy group named the Article 29 Working Party have repeated warnings about private companies' overreach into personal data. *See, e.g.*, Chris Baraniuk, *EU Watchdogs Permit Privacy Shield to Run for One Year*, BBC (July 26, 2016), http://www.bbc.com/news/technology-36893920 [https://perma.cc/SZ4S-6ASJ]; Mark Halper, *Isabelle Falque-Pierrotin: Privacy Needs to Be the Default, Not an Option*, WIRED, https://www.wired.com/brandlab/2015/06/isabelle-falque-pierrotin-privacy-needs-default-not-option [https://perma.cc/2KL4-DSC6].

take place at the global level, like the GATS, or at a regional level, such as with the TTIP, although the latter has certain advantages. A regional agreement would be easier to achieve than an agreement among all WTO members. This would be particularly true if the agreement focused specifically on digital trade without engaging with the distinct employment issues around trade in manufactured goods. Moreover, with a regional agreement and their combined market power, the United States and the EU could benefit further from this opportunity to establish global standards indirectly. Together, the United States and the EU would make a stronger counterweight to other major market players like China that have even more divergent approaches to privacy.[149]

Despite opposition to such an agreement, there are three notable benefits to considering data privacy as a trade issue in the form of a regional agreement. First, an agreement on data privacy and trade would provide clear guidelines for the enormous market of data flow across the Atlantic, acknowledging the developments in the market and technology that require such coordination. Second, the trade framework could better incorporate the benefits of attention to consumer expectations. Third, incorporation of data privacy and trade would more fully inform the difficult weighing of countervailing interests. The following discusses each benefit in turn.

1. Clarity and Uniformity

Trade standards help achieve uniformity and certainty, which benefits businesses as well as consumers. An agreement between the United States and Europe on a shared standard for privacy in data flow would improve compliance as well as enable the global market to maximize the economic and social benefits of transborder data flow.

The value of uniformity in personal data flow privacy standards is already acknowledged in both the EU and the United States. The European Commission's rationale for adopting regional standards, as stated on its website, is that data needs to flow across borders, and conflicting rules within different sovereignties would disrupt that exchange and raise concerns among consumers about their vulnerability.[150] The EU has identified uniformity as a boon to the reliability and utility of transborder data flow. In the United States, businesses' behavior demonstrates that the "protection of private information is more valuable to an industry as a whole than to any individual company. This lack of competition over privacy has fostered widespread information sharing and has supported the institutionalization of similar practices across sectors and firms."[151]

149. *See* Tourkochoriti, *supra* note 2, at 175–76.
150. EUROPEAN COMM'N, *supra* note 99.
151. Bamberger & Mulligan, *supra* note 65, at 1565.

These uniformity benefits could be expanded to the companies engaged in transatlantic trade as well. Further dialogue and agreement on terms and shared practices would give companies more clarity regarding how to comply with a streamlined set of rules. Further, an agreement could reach more companies than the Safe Harbor did or Privacy Shield framework does with its application basis. This would further enable trade between the United States and Europe, which could be beneficial for both economies.

2. Protection of Individuals

The trade framework could also address concerns about individual privacy violations. One possible approach is the consumer expectation model as a standard for data treatment, as discussed in Part I.[152] Under an FTC consumer expectation review, user norms as well as established laws bind companies.

Emphasis on consumer expectations could better avoid some of the inherent problems in a privacy regime dependent on a user's consent, as discussed in Part I. Recall that critics have queried whether consumer consent is less meaningful due to complex and changing technology and uses of data. In this context, standards based on consumer expectations may better protect consumer interests. An objective standard of consumer expectations would take pressure off of the individual to make choices to opt in or opt out of a privacy policy in which the exchange of information for a "free" service is less imbalanced. Fundamental privacy tenets could serve as a baseline for consumer expectations without needing consumers to articulate or act on these expectations explicitly.

A regional consumer expectation model may raise new challenges. For example, research found relatively little interest in consumer expectations in Germany. However, the research also indicated that companies looking to do business beyond the EU increasingly expressed interest in consumer expectations.[153] This suggests that improved access to the regional market may aid the spread of norms among companies. Also, both the EU and United States regimes already have aspects of the consumer expectations model, as seen in the EU's "legitimate interest" standard and U.S. "unfair practices" standard.[154] Building on these similar concepts could help avoid the pitfalls of a consent-based approach.[155] It has the potential to strengthen consumer expectations and lessen consumer suspicion that information will be misused.

---

152. *See id.* at 1566, 1571, 1573.

153. *Id.* at 1572 (quoting a German businessperson as saying, "how can we explain . . . [to our] employee or a customer in let's say . . . Africa why we treat him with less respect and why we treat his data less seriously just because he happens to be in Nigeria and not in Austria").

154. *See* Federal Trade Commission Act, 15 U.S.C. § 45 (2012); The Directive, *supra* note 22, art. 7(f).

155. Tene, *Privacy Law's Midlife Crisis*, *supra* note 27, at 1248.

3. Informed Balancing of Conflicting Values and Interests

Third, the trade framework would allow for deeper analysis in the balancing of conflicting interests in policy making. Currently, privacy is the dominant focus of legislation and regulation. This focus is part of the historical artifact of privacy regulations formed at the end of World War II with the purpose of limiting an overly intrusive government.[156] As the doctrine has evolved, Polonetsky and Tene advocated for the consideration of benefits, along with risks, in privacy assessments.[157] Applied to this discussion, the consideration of easier flowing trade has social and economic value that should be part of the trade negotiations. A trade standard could bring both the costs and benefits to light.

Relatedly, a trade-based approach would allow the United States and the EU to frame negotiations around common interests. Currently, the dispute revolves around the politically heated disagreement about the limits and substance of privacy regulation. Obermayr's comments reflect the entrenched—if not fully supported—belief that U.S. and EU data privacy regimes "could hardly be more different."[158] However, from a trade perspective, the United States and the EU both gain through increased data flow. Starting from points of agreement would make further collaboration seem more possible than it does in the current environment.

CONCLUSION

Incorporating trade considerations in data privacy regulation offers some advantages over the traditional framework and would help data flow more freely across borders. The United States and Europe have regulated data privacy on a jurisdiction-specific basis, despite the nature of data in the cloud, as well as the shared values and concerns between the two regions. This approach has exacerbated the perception of differences and impeded the significant benefits of transatlantic data trade to both regions.

In light of the serious countervailing interests between individual privacy and social benefits, there are demonstrated advantages to incorporating trade considerations in data privacy regulation. First, this shift would provide clear guidelines to organizations that want to be compliant. Second, a consumer expectation model could better institutionalize fundamental privacy tenets and avoid the pitfalls of individual consent where the consumer does not fully understand the agreement. Third, trade considerations would better inform the discussion regarding benefits and common interests, which in turn would lead to better rulemaking. Resolving the complexity, hurdles, and extra process in the

156. *See* COUNCIL OF EUROPE, *supra* note 10, at 46, 62, 104.
157. Polonetsky & Tene, *supra* note 52, at 26–27.
158. Wolf, *supra* note 144.

transfer of data is an important matter. A trade framework enables consensus on standards, which could enhance better privacy protection and exchange.