Title
Transatlantic Data Privacy Law

Journal
GEORGETOWN LAW JOURNAL, 106(1)

ISSN
0016-8092

Authors
Schwartz, Paul M
Peifer, Karl-Nikolaus

Publication Date
2017

Transatlantic Data Privacy Law

Paul M. Schwartz* & Karl-Nikolaus Peifer**

International flows of personal information are more significant than ever, but differences in transatlantic data privacy law imperil this data trade. The resulting policy debate has led the EU to set strict limits on transfers of personal data to any non-EU country—including the United States—that lacks sufficient privacy protections. Bridging the transatlantic data divide is therefore a matter of the greatest significance.

In exploring this issue, this Article analyzes the respective legal identities constructed around data privacy in the EU and the United States. It identifies profound differences in the two systems' images of the individual as bearer of legal interests. The EU has created a privacy culture around "rights talk" that protects its "data subjects." In the EU, moreover, rights talk forms a critical part of the postwar European project of creating the identity of a European citizen. In the United States, in contrast, the focus is on a "marketplace discourse" about personal information and the safeguarding of "privacy consumers." In the United States, data privacy law focuses on protecting consumers in a data marketplace.

This Article uses its models of rights talk and marketplace discourse to analyze how the EU and United States protect their respective data subjects and privacy consumers. Although the differences are great, there is still a path forward. A new set of institutions and processes can play a central role in developing mutually acceptable standards of data privacy. The key documents in this regard are the General Data Protection Regulation, an EU-wide standard that becomes binding in 2018, and the Privacy Shield, an EU–U.S. treaty signed in 2016. These legal standards require regular interactions between the EU and United States and create numerous points for harmonization, coordination, and cooperation. The GDPR and Privacy Shield also establish new kinds of governmental networks to resolve conflicts. The future of international data privacy law rests on the development of new understandings of privacy within these innovative structures.

Table of Contents

* Jefferson E. Peyser Professor of Law, UC Berkeley School of Law; Director, Berkeley Center for Law & Technology. The authors would like to thank the Fritz Thyssen Stiftung (Thyssen Foundation) for their research support. For their helpful comments on previous drafts, the authors thank Colin Bennett, Caroline Boisvert, Holly Doremus, Clifton B. Fels, Dennis Hirsch, Christopher Hoofnagle, Mark Gergen, Margot Kaminski, Katherine Linos, William McGeveran, Joel Reidenberg, Daniel Solove, Lior Strahilevitz, Peter Swire, and Kurt Wimmer.

** Professor of Law, University of Cologne, Cologne, Germany; Director, Institute for Media Law and Communications Law.

INTRODUCTION

Due to the significance of international flows of personal information, the stakes are high today for the European Union (EU) and the United States when it comes to data privacy law. According to one estimate, the EU–U.S. economic relationship involves $260 billion in annual digital services trade.[1] Cross-border information flows represent the fastest growing component of trade in both the EU and the United States. As one technology reporter noted, "International data transfers are the lifeblood of the digital economy."[2] Yet, differences in transatlantic regulations potentially imperil critical international data flows.[3]

In today's information economy, much of the EU–U.S. data trade involves personal data. Leading U.S. companies depend on access to and use of the personal information of EU citizens to provide data-driven services on the continent. Cloud providers, which offer decentralized mobile access to computing power throughout the world, similarly access and use the personal data of EU citizens. A threat to these data flows derives from EU doubts as to whether the United States has sufficient privacy protection. The resulting EU–U.S. dispute has been termed the "transatlantic data war."[4] This term refers to the transatlantic conflict around transfers of personal data.

The roots of this "war" are found in the differing legal approaches to information privacy in the two jurisdictions. The differences are institutional,

1. Penny Pritzker & Andrus Ansip, *Making a Difference to the World's Digital Economy*, U.S. DEP'T OF COM. (Mar. 11, 2016), https://www.commerce.gov/news/blog/2016/03/making-difference-worlds-digital-economy-transatlantic-partnership [https://perma.cc/QS9J-M3P3].

2. Robert Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, N.Y. TIMES (Oct. 9, 2015), https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html [https://nyti.ms/2py7rQX].

3. *See generally* Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy, COM(2017) 9 final (Jan. 10, 2017).

4. Henry Farrell & Abraham Newman, *The Transatlantic Data War*, FOREIGN AFFAIRS (Feb. 2016), https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war [https://perma.cc/6CGM-SMPH].

substantive, and, at the same time, elusive. Both sides recognize information privacy as an important value yet struggle to identify the meaning of core differences and the critical baseline for future collaboration. In the United States, there has been skepticism about EU privacy rights and whether they are merely disguised protectionism.[5] In the EU, there has been a longstanding debate about whether U.S. law provides sufficient protections for the personal information of EU citizens when U.S. companies and public authorities collect and process it.[6] This policy debate has been accompanied by the EU setting strict limits on transfers of personal data to any non-EU country that lacks significant privacy protections.

The restrictions are set by two EU legal mandates. The first is the European Directive on Data Protection, which permits data transfers from the EU to a third-party nation only when it has "adequate" privacy protections.[7] The second is the General Data Protection Regulation (GDPR), which will replace the Directive on May 25, 2018.[8] Under the GDPR, the adequacy requirement for data transfers continues to be the legal touchstone.[9] The EU has never considered U.S. data privacy law to have an adequate level of protection.[10] It has faulted U.S. information privacy law for its patchwork nature and lack of adequate remedies.

In response to the EU's judgment that the privacy protections of U.S. law are insufficient, the EU and the United States developed a set of first-generation solutions for transatlantic exchanges. A turning point for these mechanisms came in June 2013, with the start of Edward Snowden's revelations regarding the practices of the National Security Agency (NSA).[11] For the EU, the resulting information demonstrated that the NSA had engaged in data surveillance of EU citizens without adequate respect for their data privacy rights. The NSA's storage and analysis of bulk data pertaining to EU citizens was a major point of contention.[12]

The resulting political firestorm has either invalidated or imperiled all first-generation transatlantic data transfer mechanisms.[13] An initial second-genera-

---

5. *Id.*

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

7. Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31, 56–57 (EC) [hereinafter DP Directive].

8. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 60–62 (EU) [hereinafter GDPR].

9. *Id.* at art. 45.

10. *See, e.g.*, *Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/99*, 2 DG MARKT Doc. 5092/98, WP 15 (Jan. 26, 1999) [hereinafter Article 29 Working Party] (stating in reference to U.S. privacy law that "the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot be relied upon to provide adequate protection" for data transferred from EU).

11. The Guardian has a helpful archive relating to the leaked NSA files. *See* Ewan Macaskill & Gabriel Dance, *NSA Files Decoded*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [https://perma.cc/9MFL-835H]; James Ball, et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 6, 2013), https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [https://perma.cc/VQG5-Q44E].

12. *See infra* Section IV.A.

13. The decisive move was made in 2015 by the European Court of Justice's *Schrems* decision, which invalidated the Safe Harbor Agreement between the EU and the United States. *See generally* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (Oct. 6, 2015).

tion solution, the EU–U.S. Privacy Shield, was finalized in June 2016.[14] There are already legal challenges to it in the EU.[15]

Bridging the transatlantic data divide is, therefore, a matter of the greatest significance. On the horizon is a possible international policy solution around "interoperable," or shared legal concepts. President Barack Obama and the Federal Trade Commission (FTC) promoted this approach. For the Obama White House, there was a need for a "multistakeholder process" with the international partners of the United States to "facilitate interoperable privacy regimes."[16] These regimes were to be based on the starting point of "mutual recognition," which entailed an "embrace of common values surrounding privacy and personal data protection."[17]

The extent of EU–U.S. data privacy interoperability, however, remains to be seen. In exploring this issue, this Article analyzes the respective legal identities constructed around data privacy in the EU and the United States. It identifies profound differences in the two systems' image of the individual as bearer of legal interests. The EU has created a privacy culture around "rights talk" that serves to protect "data subjects."[18] In the EU, rights talk forms a critical part of the postwar European project of creating the identity of a European citizen. As Jürgen Habermas argues, this task is a constitutional one that is central to the EU's survival.[19] In the United States, by contrast, data privacy law is based on the idea of consumers whose interests merit governmental protection in a marketplace marked by deception and unfairness. In the United States, the focus is on "marketplace discourse" about personal information and the safeguarding of "privacy consumers."[20]

This Article uses the models of rights talk and marketplace discourse to analyze how the EU and United States protect their respective data subjects and privacy consumers. A focus of the Article is on the respective doctrines of consent and contract in the two legal systems, which reflect profoundly different

14. *See generally* Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection by the EU–U.S. Privacy Shield, C(2016) 4176 final, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf [https://perma.cc/H7JZ-LZ5D] [hereinafter Privacy Shield, Implementing Decision].

15. Peter Sayer, *A Second Privacy Shield Legal Challenge Increases Threat to EU-US Data Flows*, PC WORLD (Nov. 3, 2016), http://www.pcworld.com/article/3138196/cloud-computing/a-second-privacy-shield-legal-challenge-increases-threat-to-eu-us-data-flows.html [https://perma.cc/TDV6-8NW9].

16. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 31–32 (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/KJ6H-5XQ5] [hereinafter CONSUMER DATA PRIVACY].

17. *Id.* at 31. In similar tones, the FTC has noted, "Efforts underway around the world . . . indicate an interest in convergence on overarching principles and a desire to develop greater interoperability." FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 10 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/28ZC-HETQ].

18. *See infra* Section I.A.

19. JÜRGEN HABERMAS, ZUR VERFASSUNG EUROPAS 66 (2011).

20. *See infra* Section I.B.

perspectives. In the EU, there is a collective approach to ordering privacy. Consequently, the EU limits contract through strict requirements of necessity, purpose limitation, and a ban on "tying."[21] As for consent, it is subject to limits in the EU that make it unusable in many areas as a legal basis for personal data processing.

Where the focus of the EU is on restricting consent and contract, these doctrines are absent in U.S. data privacy law. In the absence of a requirement of a legal justification for personal data processing, parties in the United States can collect and use personal data without consent or contract.[22] Their only duty is to follow any sector laws or other mandates that might exist.

There are also likely future forces for convergence and divergence on the horizon. The forces moving the two legal systems for privacy together are a shared technological environment, increased political agreement around the benefits of personal data flow, and common security and law enforcement concerns. The forces moving the systems apart begin with the political and institutional dimensions of the EU's rights talk. There are also great differences concerning privacy remedies and a strong possibility for misunderstandings and disagreements around concepts of contract and consent in the two systems.

Finally, there are indications of a potential negative "Trump Effect" in privacy law that will divide the United States and EU in the area. President Trump can single-handedly overturn a Presidential Policy Directive that is a significant part of the Privacy Shield Framework. Moreover, his persistent, evidence-free claims of lawless surveillance of his campaign by the Obama Administration[23] can erode EU trust in the Privacy Shield's assertions about legal restrictions on surveillance on this side of the Atlantic. As a further concern, the Trump Administration may fail to tend to the necessary U.S. institutions, which the EU relies on for oversight of American privacy commitments to it.

Yet, even if there are differences between the EU and United States concerning data privacy, there is still a path forward. A new set of institutions and processes can play a central role in developing mutually acceptable standards of data privacy. This Article argues that the future of international data privacy rests not in unilateralism, whether from the EU or United States, but in these myriad new venues for collaboration. The EU and United States can "agree to disagree" about their fundamental visions for data privacy, and at the same time,

---

21. The prohibitions on "tying" forbids a data processor from linking (or "tying") the terms within a single contractual agreement to any use of personal data, beyond that which is necessary to the purpose of the contract. *See infra* Section II.B.

22. For a discussion, see William McGeveran, *Friending the Privacy Regulator*, 58 ARIZ. L. REV. 959, 977 (2016); Paul M. Schwartz, *The EU-US Privacy Collision*, 126 HARV. L. REV. 1966, 1974–75 (2013).

23. Glenn Kessler, *Fact-checking the Trumpian Spin on 'Surveillance of Trump,'* WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/news/fact-checker/wp/2017/04/04/fact-checking-the-trumpian-spin-on-surveillance-of-trump [http://perma.cc/LD6K-AM7W].

work together to permit international data transfers. Both the GDPR and Privacy Shield require regular interactions between the EU and United States to create points for harmonization. Drawing on a model from international law, this Article proposes that the GDPR and Privacy Shield alike create a new system for "coercion, persuasion, and acculturation" within the transatlantic privacy community.[24] The future of transatlantic data trade turns on developing shared understandings of privacy within these new structures.

I. DIFFERENT VISIONS OF DATA PRIVACY

This Part considers how the two systems of data privacy law envision the individual. From the perspective of an anthropologist, law is "a species of social imagination."[25] As Clifford Geertz observes, "legal thought is constructive of social realities" and not merely "reflective of them."[26] In his 1921 Storrs lecture, Benjamin Cardozo similarly observed, "There is in each of us a stream of tendency, whether you choose to call it philosophy, or not, which gives coherence and direction to thought and action."[27] This shared cultural background forms a key part of juridical decision making. He notes, "In this mental background every problem finds its setting."[28]

This Part examines how two legal orders construct contrasting "legal identities" for individuals as bearers of data privacy interests.[29] This Article finds that the EU system protects the individual by granting her fundamental rights pertaining to data protection. This language of rights creates a connection between data subjects and the EU institutions that safeguard these interests. By contrast, U.S. law protects the individual as a privacy consumer. The view is of a person as a participant in market relations. In this market-driven discourse, the individual is a trader of a commodity, namely her personal data. Because of these two versions of legal identity, the status of the individual within the respective legal systems is different. To illustrate this point, this Article compares the EU's data subject and the United States' privacy consumer across three dimensions: (1) her constitutional protections; (2) her statutory protections; and (3) her relative legal status compared to the entities that collect and process her personal data. Sections I.A and I.B examine the respective visions in the EU and United States for the individual as rights-bearer.

Before we begin, some brief points about terminology and scope are required. This Article adopts the respective terminology of each legal system in identify-

---

24. *See* Ryan Goodman & Derek Jinks, *How to Influence States: Socialization and International Human Rights Law*, 54 DUKE L.J. 621, 623 (2004) (identifying these three elements of regime design choice).

25. CLIFFORD GEERTZ, LOCAL KNOWLEDGE: FURTHER ESSAYS IN INTERPRETIVE ANTHROPOLOGY 232 (1983).

26. *Id.*

27. BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 12 (1921).

28. *Id.* at 13.

29. On the question of how law constructs a "legal identity," see James Q. Whitman, *Consumerism Versus Producerism*, 117 YALE L.J. 340, 394 (2007).

ing their similar zones of activity. Hence, when we address EU privacy law, we speak of "data protection" and refer to the similar area of U.S. law as "information privacy law."[30] When we desire a neutral term, this Article uses "data privacy law."[31]

Regarding this Article's scope, its focus is on the EU and the United States. To be sure, data privacy is a topic broader than the transatlantic relationship. In particular, there are important developments occurring throughout Asia.[32] Our exclusive attention to transatlantic developments is justified, however, on at least two grounds.

First, this relationship has traditionally set the pattern for the rest of the world. The EU–U.S. Safe Harbor is widely followed by other agreements for international data trade.[33] Second, a focus on the EU helps in understanding the basis for most other legal systems' approach to data privacy. EU data protection law has been stunningly influential; most of the rest of the world follows it. In the assessment of Graham Greenleaf, an Australian privacy expert, "[S]omething reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws."[34]

Hence, by looking at the EU, this Article examines the most influential source for the world's data privacy law. In examining U.S. information law, in contrast, this Article looks at the approach in the world's largest economy and home of the most important technology companies.[35] We now turn to the different models of the individual as rights-bearer in the two systems.

A. RIGHTS TALK IN THE EU

The EU engages in a rights-focused legal discourse centered on the individual whose data is processed. This Article uses the shorthand "rights talk" to describe this essential aspect of EU data protection law. As for the individual whose information is at stake in this process, this Article will use the term "data subject" to refer to the rights-bearer in EU data protection law.

---

30. As examples of this terminology, see generally DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW (5th ed. 2015). For a continental example, see generally AXEL VON DEM BUSSCHE & MARKUS STAMM, DATA PROTECTION IN GERMANY (2013).

31. For an early adoption of this term in a report commissioned by the European for the Commission of the European Communities, see generally PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996).

32. For a magisterial study of these developments, see generally GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS (2014).

33. *See, e.g.*, U.S. DEP'T OF COM., U.S.–SWISS SAFE HARBOR FRAMEWORK: GUIDE TO SELF-CERTIFICATION (Mar. 12, 2012) (updated Mar. 2013), https://build.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_058685.pdf [https://perma.cc/FA8W-DDWX].

34. GREENLEAF, *supra* note 32, at 57. Moreover, as Greenleaf states, "One of the most-implemented 'European' principles outside Europe is 'Data export restrictions based on destination,' which could also be named the 'adequacy requirement' for data exports." *Id.*

35. Christopher Mims, *Why 2016 Was a Watershed Year for Tech*, WALL ST. J. (Dec. 18, 2016), https://www.wsj.com/articles/why-2016-was-a-watershed-year-for-tech-1482081358 [https://perma.cc/U6ZS-YN84] (noting that five of the seven most valuable companies in the world are U.S. technology companies).

A feature of the EU is its "multilinguism." All its official documents are translated into the twenty-four languages of the member states, and all versions are of equal legitimacy.[36] In English Euro-speak, EU data protection law uniformly calls the individual whose data are processed the "data subject," and we adopt this term.[37] Linguistics also teaches us that the subject is the most prominent active agent of a sentence. In a similar fashion, the EU privileges the individual whose personal information is processed. In short, the EU uses the language of constitutional rights to promote the rights of its data subject.

Section I.A.1 below examines the rise of a European law of data privacy anchored at the constitutional level and explores the roots of this development. Section I.A.2 looks at the obligation in European data for accompanying statutory protections. Finally, section I.A.3 considers how EU law undertakes to protect not only privacy, but also the free flow of information. When other interests conflict with data privacy, EU courts undertake a proportionality analysis. It does not permit any invasion of privacy that might be carried out at a lower constitutional cost.

1. Constitutional Protections

In the EU, data protection is a fundamental right anchored in interests of dignity, personality, and self-determination. The path to creation of this right began before World War II, as different national legal systems recognized rights of dignity and personality within their constitutional law. The postwar constitutions of Italy (1947) and Germany (1949) were in the front ranks of this development.[38] From their devastating experience with fascism and Nazism, these countries drew the lesson of safeguarding human dignity. At the transnational level after World War II, and as an essential part of the creation of a postwar identity, Europeans also developed a supranational system of fundamental rights. These interests are now protected by institutions both within the EU, such as the European Court of Justice, and outside of it, such as the European Court of Human Rights.[39]

---

36. For a discussion of multilingualism in data protection law, see GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 9 (2014).

37. *See, e.g.*, DP Directive, *supra* note 7, at 33; GDPR, *supra* note 8, at 11.

38. GRUNDGESETZ [GG] [Basic Law], art. 1–2, *translation at* https://www.gesetze-im-internet.de/englisch_gg [https://perma.cc/YD36-ALBB]; art. 2–3 Costituzione [Const.] (It.).

39. For example, the European Union Charter of Fundamental Rights outlines six categories of rights which EU nations are bound to uphold: dignity, freedoms, equality, solidarity, citizens' rights, and justice. *See* Charter of Fundamental Rights of the European Union, 2000 O.J C 364/10 [hereinafter Charter]. Similarly, the European Court of Human Rights adjudicates allegations of individual or state violations of the European Convention on Human Rights, which outlines the signatories' obligation to respect human rights for all persons within their jurisdiction. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 1, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter The European Convention on Human Rights].

The trend of supranational rights in the postwar European order extends the already significant role of "constitutional politics" within European nations.[40] In the description of Alec Stone Sweet, this process involved the enactment of extensive postwar constitutional rights in Europe as well as a subsequent privileging of the judicial role in the policy-making environment.[41] The European Convention of Human Rights and the Charter of Fundamental Rights function as the two pillars of fundamental rights in Europe. The former is an international treaty; the latter is a key constitutional document of the EU.

As Frederico Fabbrini summarizes, Europe now has a "plurality of constitutional sources enshrining constitutional rights" and a "plurality of constitutional views on human rights."[42] There is also a plurality of judicial bodies, national and transnational, involved in interpreting, enhancing, and extending these different sources. To understand the relationship between these sources, a few words are necessary about certain basics of European and EU law. Within its realm, EU law supersedes the law of its member states.[43] Thus, EU law represents more than a mere international treaty with the twenty-eight EU member states as contracting parties. Rather, member states shift their sovereign powers to the EU. In turn, the EU makes use of these powers, among other ways, by issuing binding directives or regulations.[44] The directives must be transformed into national law through statutes enacted by member states. In contrast, regulations are directly applicable as statutory law in the member states. Once the EU has executed its powers, the European Court of Justice has the last word in interpreting the Charter of Fundamental Rights as well as the directives and regulations.[45]

By contrast, the European Convention of Human Rights is not part of the EU, but a normal international treaty. It binds the contracting states as part of the body of international law.[46] Yet, a significant difference with the system of international law associated with the United Nations is that the Convention has its own court system. The European Court of Human Rights decides questions

40. For the classic study of "constitutional politics" in Europe, see generally ALEC STONE SWEET, GOVERNING WITH JUDGES (2000).

41. *Id.* at 3.

42. FEDERICO FABBRINI, FUNDAMENTAL RIGHTS IN EUROPE 26 (2014).

43. *See* Basic Law, *supra* note 38, art. 23 subs. 1: "With a view to establishing a united Europe, the . . . Federation may transfer sovereign powers by a law. . . ." Regarding the sphere of EU law, see ROGER J. GOEBEL ET AL., EUROPEAN UNION LAW 151–54 (4th ed. 2015).

44. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 288, 2012 O.J. C 326/47 [hereinafter TFEU] ("[(1)] To exercise the Union's competences, the institutions shall adopt regulations [and] directives . . . [(2)] A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States . . . [(3)] A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.").

45. For an overview, see GOEBEL ET AL., *supra* note 43, at 53–64.

46. *See* The European Convention on Human Rights, *supra* note 39, at art. 1 ("The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section 1 of this Convention.").

under the Convention.[47] In a demonstration of Fabbrini's point about multiple authorities, the EU applies the Convention as far as they "constitute general principles of the Union's law."[48]

Over time, the European rights regime came to include not only privacy, but an explicit right to data protection. Both interests now have the status of a fundamental right in Europe. The European Convention of Human Rights is an international treaty drafted by the Council of Europe. In Article 8, it grants the individual a "right to respect for his private and family life."[49] The Convention established the European Court of Human Rights, which has built on Article 8 to identify specific rights regarding data protection.[50]

Within the EU, the key constitutional document is the Charter of Fundamental Rights. With the signing of the Lisbon Treaty by EU member states, the Charter became binding constitutional law for the EU in 2009.[51] It makes explicit the protections of community law for human rights and builds on the requirement, as expressed by the European Court of Justice as early as 1969, that "respect for human rights . . . is a condition of the lawfulness of Community acts."[52] The Charter protects privacy, like the Convention, and also contains an explicit right to data protection.[53] Article 8(1) provides: "Everyone has the right to the protection of personal data . . . ."[54] The European Court of Justice reaches decisions under the Charter, the Treaty, and the Human Rights Convention; the European Court of Human Rights decides cases falling under the Human Rights Convention.[55] In Fabbrini's assessment, this overlap of judicial institutions and governance layers for protecting human rights creates "an incentive for an expansion of the norms and institutions for the protection of fundamental rights."[56]

---

47. For an important study of how the decisions of the European Court of Human Rights have been received and influenced eighteen national legal orders, see Helen Keller & Alec Stone Sweet, *Assessing the Impact of the ECHR on National Legal Systems*, *in* A EUROPE OF RIGHTS: THE IMPACT OF THE EHCR ON NATIONAL LEGAL SYSTEMS 677 (Helen Keller & Alec Stone Sweet eds., 2008).

48. Consolidated Version of the Treaty on European Union art. 6, 2012 O.J. C 326/13.

49. The European Convention on Human Rights, *supra* note 39, at art. 8.

50. *See, e.g.*, *Copland v. United Kingdom*, 62617/00 Eur. Ct. H.R. at 12 (2007) (holding that collection and storage of personal information related to an individual's telephone, e-mail, and Internet usage, without her knowledge, implicated Article 8 rights); *P.G. & J.H. v. United Kingdom*, 44787/98 Eur. Ct. H.R. at 15 (2011) (holding that Article 8's protection of private life can be affected by measures that occur "outside a person's home or private premises"); *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* 931/13 Eur. Ct. H.R. at 15 (2015) (holding that extensive publication of personal, publicly available tax information constituted a violation of Article 8).

51. JEAN-CLAUDE PIRIS, THE LISBON TREATY 146 (2010).

52. *Id.*

53. *See* Charter, *supra* note 39, at art. 8(1).

54. *Id*. A right to data protection is also protected by Article 16 of the Treaty on the Functioning of the European Union. *See* TFEU, *supra* note 44, at art. 16.

55. *See* GOEBEL ET AL., *supra* note 43, at 253–58.

56. FABBRINI, *supra* note 42, at 13–14. There is some debate about the relationship of the right to privacy, as found in Article 7 of the Charter and Article 8 of the Convention, with the explicit right of data protection of Article 8 of the Charter. The European Court of Justice has combined both concepts at times in holding that EU law protects a "right to respect for private life with regard to the processing

These transnational developments have been accompanied by recognition of a constitutional right to data protection in several EU member states. These include Germany's pathbreaking "right to informational self-determination" of 1983 and its "right of trust and integrity in information systems" of 2008.[57] Other EU states with constitutional protections for data protection, whether explicitly in their national constitution or through judicial interpretation, include the Czech Republic, Greece, Hungary, Lithuania, Poland, the Slovak Republic, and Spain.[58] Here is further evidence of Fabbrini's "plurality of constitutional sources enshrining constitutional rights."[59]

As is common in Europe for constitutional rights, the EU's rights to privacy and data protection do not merely constrain the government. Although these interests require positive government action to protect individuals, they also reach private parties. In the terminology of European law, these rights have "horizontal" effects; that is, these interests reach within "private-on-private" relations as contrasted with merely "vertical" applications that concern "government-on-private" matters.[60]

The resulting European data protection system centers itself around the data subject as a bearer of rights. It views data privacy as part of its legal culture of fundamental rights. This Article uses the concept of rights talk to indicate how data protection law in Europe joins in this fundamental rights project. Indeed, the processing of personal data has long been viewed as raising significant risks to these essential interests. As the 1978 French national data protection law warns, "informatics" poses a danger to "human identity, human rights, privacy, [and] individual or public liberties."[61] Another early continental data protection statute, the German Federal Data Protection Law of 1977, began in a far less dramatic fashion. It dryly noted the risks that data processing raises to the "legitimate interests of the affected party."[62] The academic literature of that day makes clear, however, that the Bundestag, in enacting this statute, was acting in response to the threat that personal data processing raises to "personal integ-

---

of personal data." Cases C-92/09 Schecke and C-93/09 Eifert v. Land Hessen, 2010 E.C.R. 662 at ¶ 52 (Nov. 9, 2010) (establishing this critical combination). Through this language, the Luxembourg court formally constitutionalized data protection while also failing to conceptualize the relationship between the Charter's protections for privacy and data protection.

57. BVerfG, 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil) (Census Case), Dec. 15, 1983. For a summary in English, see DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 299 (2d ed.1997); *see generally* BVerfG, 1 BvR 370/07, 1 BvR 595/07, Feb. 27, 2000, *translation at* http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html [https://perma.cc/6AT3-X7LU].

58. FUSTER, *supra* note 36, at 66–70.

59. FABBRINI, *supra* note 42, at 26.

60. *See generally* Case C-144/04, Mangold v. Helm, 2005 Eur. Ct. H.R. 709 (Nov. 22, 2005).

61. Act 1978-17 of 6 January 1978, Data Protection Law, art. 1 (Fr.), *translation at* https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf [https://perma.cc/4759-7WVT].

62. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz), Jan. 27, 1977, BGBl. I at 201, *last amended by* Gesetz, Feb. 25, 2015, BGBl. I at 162.

rity."[63] In the words of the German Federal Constitutional Court in its celebrated *Census* case, data processing threatens the decisional authority of the individual as well as the existence of "a free democratic community based on its citizens' capacity to act and participate."[64]

In sum, European data protection law is strongly anchored at the constitutional level. Its goal is to protect individuals from risks to personhood caused by the processing of personal data, and its favored mode of discourse is rights talk. When it discusses privacy, it uses the language of human rights to develop protections for its data subjects.

2. Statutory Protections

As part of the obligation to protect the data subject, EU constitutional law mandates the enactment of statutory laws that regulate data use. The basic rule is that personal data processing requires a legal basis,[65] an idea which Article 8(2) of the Charter expresses by its mandate of a "legitimate basis laid down by law" for data use.[66] Processing personal data without an adequate justification in law is itself a violation of legal rights.

Moreover, the fundamental rights of the individual must be protected even in the absence of sensitive data or harm to the individual. Two recent landmark privacy decisions of the European Court of Justice make this same point: *Google Spain*, known worldwide as the "right to be forgotten" decision,[67] and *Schrems*, a similarly famous case celebrated (or condemned) as the decision that sank the Safe Harbor agreement.[68] In *Google Spain*, the European Court of Justice observed that the data subject's fundamental interests do not turn on whether "the inclusion of the information in question . . . causes prejudice to the data subject."[69] Rather, processing personal data poses an inherent threat to the rights of the data subject and, due to this risk, may only be carried out if the law permits it and shapes how the information will be used. In *Schrems*, the European Court of Justice similarly stated: "To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question . . . is sensitive or whether the

63. Spiros Simitis, *Einleitung*, *in* KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ 63 (Spiros Simitis et al. eds., 2d ed. 1979).

64. BVerfG, 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil) (Census case), Dec. 15, 1983.

65. NIKO HÄRTING, DATENSCHUTZ-GRUNDVERORDNUNG 80 (2016).

66. *See* Charter, *supra* note 39, at 2000 O.J. (C 364) art. 8. In its decision in *Schrems*, the European Court of Justice held that any EU legislation involving "interference with the fundamental rights" of privacy must "lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data." Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 91 (Oct. 6, 2015).

67. *See generally* Case C-131/12, Google Spain v. AEDP, 2014 E.C.R. 317 (May 13, 2014).

68. *See generally Schrems*, 2015 E.C.R. 650.

69. *Google Spain*, 2014 E.C.R. 317 at ¶ 96.

persons concerned have suffered any adverse consequences on account of that interference."[70]

As part of this approach, EU law proceeds by first enacting "omnibus laws."[71] Such laws seek to cover all personal data processing, whether in the public or private sector, and regardless of the area of the economy. These laws are then bolstered by sectoral laws that single out specific kinds of data processing and increase the specificity of regulatory norms.[72] As an example, data protection law has traditionally singled out telecommunications as an object for sectoral regulations.[73]

The key regulatory norms are centered around the enactment of Fair Information Practices (FIPs). These principles are found in the EU at the constitutional level as well as in statutory law. As expressed in the Charter's Article 8, the system of FIPs has six key elements: (1) a requirement of fair processing; (2) a requirement of processing for specified purposes; (3) a requirement of consent or other legitimate basis for processing; (4) a right of access to data; (5) a right to have data rectified; and (6) a requirement of independent data protection authorities checking compliance with these rules.[74]

The main reference point for European data protection law will soon be the General Data Protection Regulation (GDPR) of 2016.[75] The current key regulatory document, one that the GDPR will replace, is the European Data Protection Directive of 1995.[76] The GDPR takes effect on May 25, 2018, which will mark a decisive moment for international privacy law.[77] Both the Directive and the GDPR express all these FIPs.

Moreover, the decision to replace the Data Protection Directive with a regulation demonstrates the rising significance of EU information privacy as a statutory matter. Enacted in 1995, the Data Protection Directive, like other EU directives, is a "harmonizing" instrument, which means that it is not directly binding on member states.[78] The Directive required enactment of national legislation that reflected its strictures. In contrast, a regulation does not require harmonizing legislation for it to take effect; it creates directly enforceable standards.[79] The EU's recourse to a regulation follows from its recognition of privacy as a human right and the high status of the data subject. As noted above,

---

70. *Schrems*, 2015 E.C.R. 650 at ¶ 87.

71. For a discussion, see SOLOVE & SCHWARTZ, *supra* note 30, at 1096.

72. *Id.*

73. *See* art. 1 subs. 2 with Recital 4 of Directive 2002/58/EC of 12 July 2002, 12 July 2002, 2002 OJ (L 201) 37 [hereinafter ePrivacy-Directive]; GDPR, *supra* note 8, at art. 95 with Recital 173.

74. Schwartz, *supra* note 22, at 1974–75.

75. *See generally* GDPR, *supra* note 8.

76. *See generally* DP Directive, *supra* note 7.

77. GDPR, *supra* note 8, at art. 99.

78. Schwartz, *supra* note 22, at 1971–72.

79. *Id.* at 1992–93. The lack of uniformity throughout the EU under the Directive represented a relative failure for that policy instrument. *Id.* at 1993. The EU's choice to enact a Data Protection Regulation, rather than a new Directive, reflects the widespread dissatisfaction with the resulting privacy norms of EU member states.

cornerstone documents of European integration safeguard privacy and data protection as human rights.[80] In a reflection of the data subject's high status, the GDPR provides directly binding statutory protection in EU law for her. This choice marks a notable change with the established path of EU consumer protection law, where the usual path has been to enact directives, and not regulations, to protect citizens.[81]

European Law also supplies a definite path to legal protection following harms to the data subject. Such a remedy does not depend on harm to a monetary or property interest when personal information is misused.[82] Both the data subject and a data protection authority can request an injunction to stop a practice that harms a privacy interest and can receive damages based on a nonmaterial injury in cases of a serious invasion of one's protected sphere of privacy.[83] Continuing this approach, the GDPR explicitly allows for compensation for both "material or non-material damage" following a failure to fulfill its requirements.[84]

In short, European data protection law requires statutory laws as a constitutional matter. These laws begin with omnibus laws, which receive further specification through targeted laws. No areas are left unregulated, and data subjects are guaranteed remedies for privacy harms.

3. Data Subject Versus Data Processor

Like other rights in the EU system, data protection is not boundless. Nonetheless, EU law grants its data subjects a privileged position in various legal texts, including in its foundational documents. Article 52(1) of the European Charter permits limitation of "rights and freedoms" but requires that such restrictions "be provided for by law and respect the essence of those rights and freedoms."[85] In the first part of Article 52(1), the Charter requires a legal basis, such as a statutory provision, for limiting a right.[86] The second part of Article 52(1) then creates a guarantee of protection for "the essence," or core, of rights and freedoms.[87] This language means that the core part of each right must be free from alteration or intrusion, whether through legislation or other means. In turn, one of the most important roles of the European judiciary is to identify and safeguard the essence of the Charter's rights.

---

80. For an early exploration of the human rights backdrop of EU data privacy law, see Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1349–50 (2000).

81. The approach of these directives has been termed one of "minimum harmonisation." STEPHEN WEATHERILL, EU CONSUMER LAW AND POLICY 317 (2d ed. 2013).

82. JAN PHILIPP ALBRECHT & FLORIAN JOTZO, DAS NEUE DATENSCHUTZRECHT DER EU 126–29 (2017).

83. 128 BGHZ 1381, 1995, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 1998, 1381 (Ger.).

84. GDPR, *supra* note 8, at art. 82(1).

85. Charter, *supra* note 39, at art. 52(1).

86. *Id.*

87. *Id*.

To be sure, EU law safeguards not only privacy and data protection, but also the free flow of information. It does so as part of its goal of establishing an internal market for personal data in which there is "free movement of goods, persons, services and capital," as the Data Protection Directive expressed in 1995.[88] The twin goals, then, are to ensure both a free flow of personal data from one member state to another and high standards of data protection to protect "the fundamental rights of individuals."[89] As a Recital to the Directive states, "in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States."[90] The plan is to establish high shared levels of data protection in all member states and then to require a free flow of information throughout the internal market. Such a goal is "vital to the internal market."[91]

There is also recognition here of the monetary value of international flows of information. The EU has a longstanding interest in economic liberalization of trade and in access to the global information economy. In the view of Johannes Masing, a law professor and Justice on the Federal Constitutional Court of Germany, "[U]nhindered economic transactions are of the greatest importance for the future of Europe."[92] The EU's own Digital Market Initiative and related project for a directive on contracts for digital contracts all demonstrate an awareness that the EU has much to gain from rules that promote advanced technology and related services.[93]

Beyond the Directive and the Digital Market Initiative, the EU's treaties recognize the value of the flow of information. Most importantly, Article 16(2) of the Treaty on the Functioning of the European Union refers to the "free movement" of personal data and brings it within the scope of EU law.[94] Outside of its data protection policy framework, the EU's interest in the free flow of information forms part of its landmark legal initiative to create a digital single market in the EU.[95] Other interests recognized by EU law that can conflict with data protection include the right to access information, freedom of expression, and journalistic freedoms. Article 11 of the Charter of Fundamental Rights protects these interests.[96]

---

88. DP Directive, *supra* note 7, at Recital 3.

89. *Id.*

90. *Id.* at Recital 8.

91. *Id.*

92. Johannes Masing, *Herausforderungen des Datenschutzes*, 2012 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 2305, 2310 (2012).

93. For an overview of the Digital Single Market strategy of the EU, see European Commission, *Digital Single Market*, EUROPA, https://ec.europa.eu/digital-single-market [https://perma.cc/7YB5-22XU].

94. *See* TFEU, *supra* note 44, at art. 16(2). Similarly, the GDPR recognizes both goals. It splits its Article 1 between the goal of "protection of natural persons with regard to the processing of personal data" and "rules relating to the free movement of personal data." GDPR, *supra* note 8, at art. 1.

95. European Commission, *supra* note 93.

96. Charter, *supra* note 39, at art. 11.

When these other interests conflict with data protection, EU courts undertake a proportionality analysis. Alec Stone Sweet has shown how this test became a firm part of postwar European constitutional law. He depicts it as consisting of a "'least-means' test."[97] The idea is that "it is never constitutionally sufficient . . . that the constitutional benefits outweigh the constitutional costs; instead, the benefit must be achieved at the least constitutional costs (least means)."[98] The European Charter of Fundamental Rights adopts the proportionality test for restrictions on any of its fundamental interests in its Article 52(1).[99] In the EU's proportionality analysis, there is no privileging of information flow and of the other interests that might trump invasions of data protection. The question is whether the law's protection of another relevant interest can be carried out at a lower constitutional cost to privacy.[100] In *Google Spain*, for example, the European Court of Justice identified a data privacy interest in delisting of search engine results.[101] The necessary test looked to whether the information listed on the webpage was "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing . . . by the operator of the search engine."[102] The term "excessive" in the opinion is a classic hallmark of proportionality analysis.

Data protection law does not concern itself greatly with how its protection of the data subject might negatively impact useful activities of data processors.[103] In this regime, economic interests in information and benefits on the "supply side" regarding technology are not especially important. The European Court of Justice's decision in *Google Spain* demonstrates this aspect of EU data protection law. As the European Court of Justice observed in that decision, "the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data."[104] The Luxembourg Court felt that "[i]n the light of the potential seriousness of the interference" with those interests, "it cannot be justified by merely the economic interest which the operator of such an engine has in that processing."[105] Free flow of information matters, but not as much, ultimately, as the safeguarding of dignity, privacy, and data protection in the European rights regime. We now turn to the privacy consumer of U.S. information privacy law.

---

97. SWEET, *supra* note 40, at 98.

98. *Id.*

99. *See* Charter, *supra* note 39, at art. 52(1). For use of this test in a privacy case, see generally Case C-291/12, Schwarz v. Bochum, 2013 E.C.R. 401 (June 13, 2013).

100. SWEET, *supra* note 40, at 98–99.

101. Case C-131/12, Google Spain v. AEDP, 2014 E.C.R. 317, ¶ 88 (May 13, 2014).

102. *Id.* at ¶ 94.

103. Thus, the GDPR speaks of the importance of "the free flow of personal data within the Union and the transfer to third countries and international organisations." GDPR, *supra* note 8, at Recital 6. But it does so within the context of the requirement for "a high level of the protection of personal data." *Id.* The GDPR also notes that data subjects are to have "control of their own personal data" *Id.* at Recital 7.

104. *Google Spain*, 2014 E.C.R. 317, at ¶ 80.

105. *Id.* at ¶ 81.

B. MARKETPLACE DISCOURSE IN THE UNITED STATES

Where the EU views its laws as reflecting and making concrete the broader mandates of a fundamental privacy right, the United States anchors its information privacy law in the marketplace. Unlike the EU's data subject, U.S. law does not equip the privacy consumer with fundamental constitutional rights; rather, she participates in a series of free exchanges involving her personal information. In this legal universe, the rhetoric of bilateral self-interest holds sway. Personal information is another commodity in the market, and human flourishing is furthered to the extent that the individual can maximize her preferences regarding data trades. The focus of information privacy law in the United States is policing fairness in exchanges of personal data.

The marketplace discourse that is central to U.S. privacy law begins in terms of the identification of the individual whose interests are protected. In referring to the party whose personal data are processed, many U.S. privacy laws use the term "consumer."[106] Other laws identify the individual based on a specific consumer relationship.[107] These statutes all situate the individual squarely in marketplace relations, whether as a consumer, customer, or "subscriber" of telecommunications. In a nod to this dominant language, this Article refers to a bearer of privacy interests in the United States as the "privacy consumer."

Section I.B.1 below considers the marked limitations of any constitutional protections for information privacy compared to those present in European law. Section I.B.2 evaluates the patchwork approach to statutory protection in the United States, which leaves notable gaps. Moreover, the logic of marketplace discourse, rather than rights talk, is dominant in this legal landscape. Finally, section I.B.3 considers the strong protections in U.S. law for the free flow of information. The U.S. legal system favors its data processors over its privacy consumers. There is no equivalent in the United States to the EU's fundamental right to data protection and no constitutional requirement in the United States that data processors have a legal basis for any use of personal data.

1. Constitutional Protections

Our analysis begins with the private sector. There is no constitutional right to information privacy in the United States analogous to the EU's right to data protection. The U.S. Constitution does not extend to "horizontal-to-horizontal," or private, relations that are purely among private individuals.[108] Moreover, the Constitution does not oblige the government to take positive steps to create

106. Such laws include the Fair Credit Reporting Act, *see* 15 U.S.C. § 1681 (2012) (FCRA); Gramm–Leach–Bliley Act, *see* 15 U.S.C. §§ 6801–6809 (2012) (GLBA); and Video Privacy Protection Act, *see* 18 U.S.C. § 2710 (2012) (VPPA).

107. For example, the Cable Act speaks of "subscribers," *see* 47 U.S.C. § 551(a) (2012), and the Telecommunications Act of "customers," *see* 47 U.S.C. § 222(a) (2012).

108. *See* GEOFFREY R. STONE ET AL., CONSTITUTIONAL LAW 1543 (7th ed. 2013); Frank I. Michelman, *The State Action Doctrine*, *in* GLOBAL PERSPECTIVES ON CONSTITUTIONAL LAW 228 (Vikram David Amar & Mark V. Tushnet eds., 2009).

conditions to allow for the existence of fundamental rights.[109] Frank Michelman traces this orientation back to an American fear of oppression from governmental power as well as the goal of the U.S. Constitution to create a government of only limited powers.[110]

In the public sector, there is only a limited interest in information privacy in the United States that protects individuals when the government processes their personal data. The two most important sources of this interest are the Fourth Amendment and the Due Process Clause of the Fourteenth Amendment. The Fourth Amendment protects individuals against certain kinds of collection of personal information by the government. It safeguards a right of the people to be secure against searches of "persons, houses, papers and effects."[111] But in their role limiting governmental activities, these interests are greatly limited as a source of data privacy rights.

The Fourth Amendment is concerned only with searches and their reasonableness or unreasonableness. It proves a poor fit with the conditions of modern governmental use of personal data in routinized databases that administer public benefits and services. In drawing on information already in its databases, the government's action is not limited by a constitutional concept that first requires a search or seizure.[112] Under the precedent of the Supreme Court, moreover, the Constitution does not protect the individual when a "third party," such as her bank, surrenders her personal information to the government.[113] At best, the Fourth Amendment provides a judicially enforced warrant requirement against a limited group of law enforcement activities.

As for the Fourteenth Amendment, the Supreme Court used it in *Whalen v. Roe* to identify a general right to "information privacy."[114] Almost four decades after the Supreme Court articulated the *Whalen* interest, both its existence and its reach remain uncertain.[115] At least one court has expressed "grave doubts" about whether this interest is more than mere dicta from the 1977 decision.[116] In its most recent case concerning the right to information privacy, the Supreme

109. Deshaney v. Winnebago Cty. Dep't of Soc. Servs., 489 U.S. 189, 196 (1989).

110. Michelman, *supra* note 108, at 228.

111. U.S. CONST. amend. IV.

112. This idea could be called the "first-party doctrine" as opposed to the "third-party doctrine." *See generally* Smith v. Maryland, 442 U.S. 735 (1979), which establishes the third-party doctrine. As for the first-party doctrine, courts will only consider whether an initial "search" implicated the Fourth Amendment, not its further use. The first-party doctrine's impact has been felt in the context of data mining. *See* Paul M. Schwartz, *Regulating Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology*, 53 WM. & MARY L. REV. 351, 356 (2011).

113. *See Smith*, 442 U.S. at 742–46.

114. 429 U.S. 589, 605–06 (1977).

115. For an account of this uncertain status and the weakness of the existing *Whalen* doctrine such as it may exist, see Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 574–82 (1995).

116. Am. Fed'n of Gov't Emps., AFL–CIO v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997). Other courts have held that the right to information privacy protects only a small set of rights that can be deemed "fundamental." *See* J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981).

Court proved unwilling to resolve doubts concerning the right's viability. In *NASA v. Nelson*, in ruling against the plaintiff, the Supreme Court stated that it merely assumed the existence of the *Whalen* right "without deciding" the matter.[117] As developed in caselaw in the federal circuits, the constitutional right to information privacy protects against the state's use of personal information when such processing is made without "an express statutory mandate, articulated public policy, or other recognizable public interest."[118] The resulting constitutional scrutiny by federal courts tends to be undemanding.[119] Compared to the EU, the United States lacks any analogous right to data protection and informational self-determination.[120]

The most significant constitutional safeguards for information in the United States concern the free flow of data, not personal privacy. The two provisions of significance are the First Amendment's free speech clause and Article III's requirements for standing. Data processors are already using the First Amendment to stop or narrow information privacy laws. In *Sorrell v. IMS Health Care*, for example, the Supreme Court invalidated a Vermont law that prevented pharmacies from selling prescriber-identifying information without the consent of the prescribing party.[121] For the Court, this law failed to meet "heighted judicial scrutiny" under the Free Speech Clause because of its restriction of "[s]peech in aid of pharmaceutical marketing."[122] The First Amendment is likely to be an increasingly fertile source of rights for data processors in other areas of the economy. In an illustration of this point, Chris Hoofnagle warns that the Fair Credit Reporting Act (FCRA), a cornerstone of U.S. privacy law, "lies in tension with modern First Amendment jurisprudence" due to its restrictions on information that come from public records.[123]

Constitutional requirements for standing in the United States provide a notable obstacle for privacy consumers. Without concrete harm, there is no "case or controversy" under Article III that would permit recourse to the judicial system.[124] Yet, U.S. law has long struggled with conceptualizing the kinds of harms that violate privacy interests. Joel Reidenberg memorably expresses the problem as one of "privacy wrongs . . . in search of remedies."[125] The law in the United States remains uncertain about whether a variety of information process-

117. 562 U.S. 134, 138 (2011).

118. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980). Of the cases recognizing a *Whalen* interest, the Third Circuit decision in *Westinghouse* has been the most influential.

119. *See, e.g.*, Tucson Woman's Clinic v. Eden, 379 F.3d 531, 551 (9th Cir. 2004); Bloch v. Ribar, 156 F.3d 673, 684 (6th Cir. 1998); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983). For an overview of the caselaw, see SOLOVE & SCHWARTZ, *supra* note 30, at 565–81.

120. Schwartz, *supra* note 112, at 381–87.

121. 564 U.S. 552, 557 (2011).

122. *Id.*

123. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 286 (2016).

124. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155 (2013).

125. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877 (2002).

ing practices are "wrongs," that is, whether these practices constitute enough of an injury to consumers to merit legal remedy.

The Supreme Court has also begun to establish constitutional parameters for standing in information privacy cases. In *Spokeo, Inc. v. Robins*, the Supreme Court decided that Article III created a mandate for "a concrete harm" even when a privacy statute allowed actions for violation of its provisions and provided liquidated damages for recovery.[126] Spokeo, the defendant in that case, operates a website that allows users to search for data about individuals. Robins, who filed a class action complaint against Spokeo, argued the company qualified as a "consumer reporting agency" that was obliged to follow the requirements of the FCRA.[127] Robins also alleged that Spokeo willfully failed to comply with its legal obligations under this statute. Robins could also point to the FCRA's favorable provisions for liquidated damages when a consumer reporting agency failed to provide "reasonable procedures to assure maximum possible accuracy of" consumer reports, to provide access to consumer reports, to restrict the circumstances in which it provided reports for employment purposes, and other statutory requirements.[128]

By a 7–2 vote, the *Spokeo* Court declared that notwithstanding these allegations of a statutory violation in the case before it as well as a statutory recovery mechanism through liquidated damages, Article III required a plaintiff to do more. The requirement was to demonstrate an "injury in fact" that needed to be "concrete and particularized."[129] Unless Robins could show more than a "bare procedural violation" of a statute, the Constitution would bar any recovery.[130] He needed to demonstrate a concrete privacy harm resulting from Spokeo's shortcoming under the FCRA.[131] This constitutionalization of privacy harms represents an invitation to federal courts to rewrite and narrow the privacy statutes that allow statutory damages.[132]

2. Statutory Protections and Marketplace Discourse

Unlike EU law, U.S. law starts with a principle of free information flow and permits the processing of any personal data unless a law limits this action. There is also no requirement for the creation of statutory laws. When it does

126. 136 S. Ct. 1540, 1550 (2016).

127. *Id.* at 1546.

128. Fair Credit Reporting Act, 15 U.S.C. § 1681e(b) (2012).

129. *Spokeo*, 136 S. Ct. at 147. Six justices joined the majority opinion, and Justice Clarence Thomas filed a separate opinion concurring in the majority opinion. On the origins of this test, see *Friends of the Earth, Inc. v. Laidlaw Envt'l. Servs. Inc.*, 528 U.S. 167, 180–81 (2000), and *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

130. *Spokeo*, 136 S. Ct. at 1549.

131. The majority opinion did leave open the possibility that a "risk of real harm" can satisfy the requirement of real harm. *See id.* On remand, the Ninth Circuit did find that Robins had alleged inaccuracies by Spokeo concerning "his age, marital status, educational background, and employment history" that could be deemed a real harm to his employment prospects. Robins v. Spokeo, 867 F.3d 1108, 1111 (9th Cir. 2017).

132. For a summary of these statutes, see SOLOVE & SCHWARTZ, *supra* note 30, at 194–96.

apply, moreover, U.S. law does not protect the individual through an omnibus law. Rather, information privacy law takes the form of a patchwork that includes statutes as well as regulations at both the federal and state level. The initiation of legislative action also frequently requires the presence of a "horror story," that is, convincing evidence of abusive data practices.[133]

In contrast to the EU's conception of statutory law as embodying a fundamental privacy right, the United States situates its information privacy law in the realm of the market. Marketplace discourse and its logic are dominant. As an illustration, the mission of the FTC, the long established "privacy cop" in the United States, is "to protect consumers and promote competition."[134] It acts to prevent "unfair or deceptive acts or practices in or affecting commerce."[135]

Beyond these agencies, U.S. statutory law also reflects a marketplace orientation by favoring laws that privilege notice and consent. Privacy consumers are to be given information and then allowed to decide whether to agree to data trades.[136] Sectoral laws in the United States envision the individual narrowly within a specific marketplace relationship: as a person who wishes to obtain credit (FCRA), participate in transactions with a financial institution (Gramm–Leach–Bliley Act (GLBA)), or watch videos (Video Privacy Protection Act (VPPA)).[137] As a further example, federal health privacy protections extend only to patients receiving health care from entities engaging in electronic transmission of information for insurance reimbursement and other covered purposes.[138] For another example, and one from state law, the California Online Privacy Protection Act (CalOPPA) only applies to consumer websites and only grants rights to consumers.[139] In short, U.S. information privacy law conceives privacy interest protections as being embedded within specific marketplaces and specific consumer relationships.

The Obama White House provided final examples of marketplace discourse around privacy. Its 2012 report, *Consumer Data Privacy in a Networked World*, focused on the role of "consumers' trust in the technologies and companies that

133. On the importance of such "outside events" opening a "policy window" for privacy, see PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 199 (1995).

134. *What We Do*, FTC, https://www.ftc.gov/about-ftc/what-we-do [https://perma.cc/VZ53-9LJC].

135. 15 U.S.C. § 45(a)(1) (2012).

136. *See infra* Section III.A.

137. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012) (framing the FCRA's purpose as essential for consumers needing "fair and accurate credit reporting"); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(a) (2012) (framing the GLBA's scope as between "financial institution[s]" and "customers"); Video Privacy Protection Act, 18 U.S.C. § 2710(a)(1) (defining "consumer" under the VPPA as "any renter, purchaser, or subscriber of goods or services from a video tape service provider").

138. Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-1(a)(3) (2003) (providing that the standards of the Act shall apply to any "health care provider who transmits any health information in electronic form in connection with" standard transactions).

139. *See* CAL. BUS. & PROF. CODE § 22575(a) (2017) (defining CalOPPA's scope as only extending to "individual consumers"); *id.* § 22577(c) (limiting CalOPPA's application to websites and online services "operated for commercial purposes").

drive the digital economy."[140] In it, the White House noted the positive role of data trade and the governmental role in "promoting innovation."[141] The report emphasized how "personal data fuels an advertising marketplace that brings many online services and sources of content to consumers for free."[142]

Without the safety net of an omnibus law, this approach leaves significant areas of personal data use free from legal constraints. As an example of such an unregulated area of personal information processing, the FTC has detailed the practices of "data brokers" and how this industry circulates its information with scant transparency and free of legal oversight.[143] As its 2014 report on this industry stated, "Data brokers collect data from numerous sources, largely without consumers' knowledge."[144]

3. Privacy Consumer Versus Data Processor

In the EU, the interests of the processors of personal data are subject to a proportionality test and a least-means approach when they infringe upon privacy rights. In the United States, in contrast, the strongest constitutional protections are not for the individuals whose data are at stake, but data processors. The United States lacks any equivalent to the EU's fundamental right to data protection. Furthermore, the United States lacks any constitutional mandate requiring that data processors have a legal basis for use of personal data.

In the tug-of-war between individuals and data processors, information privacy law in the United States is broadly solicitous on the supply side in a way that EU data protection law has never been. Policymakers have long been entranced by the positive economic impact of technology companies and sought to actively protect their growth.[145] The rights-bearer of U.S. information privacy is a consumer who benefits from the presence of innovative technologies and merits protection from market failures.

This orientation has been present from the start of the Internet's commercialization, which occurred during the Clinton Administration. First and foremost, the American approach has sought to create a regulatory environment to promote the growth of technology companies.[146] As part of this inclination, there has been a long reliance on industry self-regulation. The early importance of

---

140. CONSUMER DATA PRIVACY, *supra* note 16, at 1.

141. *Id.*

142. *Id.* at 5.

143. FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/X6J2-GZZA].

144. *Id.* at 46. The report noted that one data broker alone "add[ed] three billion new records each month to its databases." *Id.* at 46–47.

145. Part of this policy orientation is also driven by an ideology that Evgeny Morozov terms "Internet-centrism," which "has become something of a religion" in the United States. *See* EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 62 (2013).

146. For a discussion of the Senate Commerce Committee's concern of the potentially negative economic impact of privacy legislation on e-commerce committees, see Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2086 (2004).

this aim was established by an influential 1997 Commerce Department compilation of papers regarding industry self-regulation of privacy in the information age.[147]

Solicitude for the supply side continued to be a central part of the U.S. privacy landscape during the Obama Administration. As noted, the Obama White House sought to further consumer trust "while promoting innovation."[148] Its goal was for this policy to spread globally; the White House hoped that U.S. leadership in "consumer data privacy [could] help establish more flexible, innovation-enhancing privacy models among our international partners."[149] Under the Trump Administration, this concern for the supply side is likely to continue. As an early indication of it, the Republican-led Congress has rolled back strong privacy protections from the Federal Communications Commission (FCC). The rules sought to extend the FCC's privacy protection to ISPs, formally termed "broadband Internet access services."[150] Overturning these FCC protections, President Donald Trump signed the joint congressional resolution, enacted pursuant to the Congressional Review Act, on April 3, 2017.[151]

Less clear, however, is the extent to which the Trump Administration will share the previous president's interest in the global dialogue around privacy. We discuss the possibilities of a "Trump Effect" in this area below at section IV.D.2. The risk is that President Trump will drive the EU and United States apart rather than together in the area of data privacy. This Article next examines how the EU and United States currently operationalize their visions of rights talk and the privacy consumer. It contrasts the EU's collective approach to private ordering and the United States' policing of the marketplace through statutes and the FTC's enforcement actions. Despite the differences that Parts III and IV set out, this Article will also identify a future path for the EU and United States to generate shared norms of data privacy.

II. THE EUROPEAN UNION: RIGHTS TALK IN ACTION

European data protection law is now chiefly expressed in the Data Protection Directive of 1995 with the countdown underway to the GDPR, which takes effect on May 25, 2018. This date will mark a decisive moment for international privacy law.[152] As Jan Albrecht and Florian Jotzo observe, the GDPR on that date will "represent without any doubt the most important legal source for data protection."[153] In proof of this significance, Albrecht and Jotzo point to the Regulation's central role in "the largest domestic market in the world," the EU,

147. U.S. DEP'T OF COM., PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997).

148. *See* CONSUMER DATA PRIVACY, *supra* note 16, at 1.

149. *Id.* at 5.

150. FCC, Notice of Proposed Rulemaking 2500, 2506 FCC 16-39 (Apr. 1, 2016).

151. The Congressional Review Act permits Congress to overturn new federal regulations by passage of a joint resolution. 5 U.S.C. § 801 (1996).

152. GDPR, *supra* note 8, at art. 99.

153. ALBRECHT & JOTZO, *supra* note 82, at 7.

as well as its future international impact.[154] Albrecht is in a good position to comment on the GDPR; as a member of the EU Parliament, he served as the influential Rapporteur of the Regulation.[155]

This Part will begin by looking at the privacy interests that the EU takes "off the table" from the legal mechanisms of contract and consent. In this fashion, this legal system adopts a collective approach to private ordering. It places a core of important data protection interests beyond the ability of a person to exchange or barter; it does so because it fears that such individual actions would erode autonomy and have a negative collective impact. This Part concludes with an examination of how the GDPR strictly cabins its doctrines of contract and consent.

A. A COLLECTIVE APPROACH TO PRIVATE ORDERING

Contract and consent are personalized legal mechanisms that allow individual expression of will. The continental legal tradition has long valued contract and consent and uses them to further individual self-determination. In its data protection law, however, the EU takes a collective approach to these doctrines.[156] One way to assess the EU's collective approach to data protection is to consider the areas that it excludes from contract and consent. A useful benchmark in this regard is that of the "information privacy inalienability." In Susan Rose-Ackerman's definition, an inalienability is "any restriction on the transferability, ownership, or use of an entitlement."[157] An information privacy inalienability, an idea developed by one of the authors of this Article, is a restriction on the transferability, ownership, or use of personal data.[158] Such restrictions may be contrary to an individual's wishes.

An information privacy inalienability restricts an individual's ability to do whatever she wishes with her data, including through contract or consent. It creates zones of noncontract and nonconsent.[159] EU data protection law establishes important areas of inalienable privacy, setting out bedrock data protection principles that are not subject to individual waiver and cannot be traded away in bargained-for exchanges.[160] Some of these restrictions are embedded at the constitutional level, others at the statutory level.

---

154. *Id.*

155. For his homepage at the European Parliament, see MEPs, Jan Philipp Albrecht, http://www.europarl.europa.eu/meps/en/96736/JAN+PHILIPP_ALBRECHT_home.html [https://perma.cc/6YRB-ZZAU].

156. A similar collective perspective is present in the EU as well regarding other aspects of contract and consent outside of data protection law, but our focus is on privacy.

157. Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931, 931 (1985).

158. Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269 (2005); Schwartz, *supra* note 146, at 2095–113.

159. Schwartz, *supra* note 146, at 2095–100.

160. *See, e.g.*, ALBRECHT & JOTZO, *supra* note 82, at 72 (noting core protections in data protection law that the individual cannot sell or exchange).

What then is "off the table" for consent and contract in the EU? The key legal move is to connect the *right* to data protection with the requirement for the creation and maintenance of *a legal system* of data protection. As Article 8 of the Charter states, personal data processing requires "a legitimate basis laid down by law."[161] The Charter sets out the full range of rights guaranteed to everyone living in the EU; it provides the EU's overarching framework of human rights, including a right to legal mechanisms for data protection. In a reflection of this requirement, the European Court of Justice has noted the need for legislation to "lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards."[162] Such legislation is constructed with the building blocks of Fair Information Practices.[163] These principles express duties and responsibilities for entities that process personal data and describe rights that people should have regarding the use of their personal information.[164] In the EU, the resulting interests in data protection are protected in their "essence" against decisions by the individual that would restrict them. As Albrecht and Jotzo note, "the data subject cannot through consent 'sell'" fundamental rights protected by the Charter, including the fundamental interests in privacy and data protection.[165]

Limits are placed by EU law on the individual's ability to trade in or surrender these rights because of their function preserving democratic self-rule. Self-determination protects autonomy. But the selling and transferring of personality rights by a data subject can alienate these interests in a fashion that makes her an object for the data processor. EU data protection law puts a core of important data privacy rights beyond the ability of a person to trade because such individual behavior would both erode a capacity of self-determination and have a negative collective impact.

EU law expresses its data privacy principles at the constitutional level as well as in regular law. As noted above, the Charter's Article 8 expresses six principles: (1) the requirement of fair processing; (2) the requirement of processing for specified purposes; (3) the requirement of consent or a legitimate basis for processing; (4) a right of access to data; (5) a right to have data corrected; and (6) the requirement of independent data protection authorities checking compliance with these rules.[166] The EU and its member states are to protect these fundamental rights by enactment of laws that provide additional particulars regarding these interests. As part of this further precision of the Charter's Article 8, the EU enacted the GDPR, which similarly relies on an expression of privacy principles to create a nonwaivable core of safeguards. The GDPR's key

161. Charter, *supra* note 39, at art. 8.
162. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 91 (Oct. 6, 2015).
163. Schwartz, *supra* note 22, at 1976.
164. *Id.*
165. ALBRECHT & JOTZO, *supra* note 82, at 72.
166. Charter, *supra* note 39, at art. 8.

expression in this regard is its Article 5.[167] There is also strong continuity here with the 1995 Data Protection Directive, which sets out its version of non-waivable safeguards in its Article 7.[168]

The list of key principles in the GDPR's Article 5 is more detailed than in the Charter's Article 8. The principles of the GDPR begin by requiring that information be: (1) "processed lawfully, fairly and in a transparent manner" (lawfulness, fairness, and transparency) and that it be (2) "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (purpose limitation).[169] The list continues with requirements of (3) data minimization; (4) data accuracy; (5) limited storage; (6) integrity; (7) data security; and (8) accountability for the data controller.[170] Finally, in Article 51, the GDPR contains strong protections for (9) independent data protection authorities.[171]

Regarding inalienabilities, there is no "freedom" of consent or contract that trumps the GDPR's fundamental rules. In the analysis of Niko Härting, "[e]ven if consent makes data processing legitimate," the "data minimization" principle of Article 6 "may make it unlawful."[172] Christopher Kuner makes a similar point in analyzing the EU's regulation of international transfers of data. These rules are secondary to the requirement of a legal basis for the processing of information. Kuner observes: "[C]ompanies become almost mesmerized with the mechanism to provide an adequate legal basis for the transfer, while neglecting to ask themselves what the legal basis is for the processing in the first place."[173] He adds: "Providing a legal basis for data processing is not a specific action, but rather an important principle that should be kept in mind at all stages of the company's compliance programme."[174]

Rights talk about data subjects in the EU is thus made through a collective orientation that removes certain powers from data subjects. Rights talk also has an impact at the institutional level. The constitutional order safeguards certain legal institutions, ones whose goals are to serve and protect the rights of the individual. The Charter grants the European Court of Justice, as ultimate interpreter of EU law, a central role in developing the rights to privacy and data protection law.[175] The Charter also explicitly protects data protection authorities and assigns constitutional rank to their independent status. It spells out their

167. GDPR, *supra* note 8, at art. 6.
168. DP Directive, *supra* note 7, at art. 7.
169. GDPR, *supra* note 8, at art. 6.
170. *Id.*
171. *Id.* at art. 51.
172. HARTING, *supra* note 65, at 26.
173. CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 242 (2d ed. 2007) (emphasis omitted).
174. *Id.*
175. *See* Charter, *supra* note 39, at Preamble (noting that the Charter affirms rights that result from the case law of the Court of Justice of the European Communities and of the European Court of Human Rights).

general tasks and, in turn, grants them constitutional authority when executing them. The European Court of Justice has already developed important caselaw devoted to the constitutional elements of independence for data protection authorities.[176]

The GDPR builds on the Charter's safeguarding of institutions that provide collective protection for privacy rights. It requires member states to provide for a "supervisory authority" and a national data protection commission, and mandates "complete independence" for this entity in "performing its tasks and exercising its powers in accordance with this Regulation."[177] It sets out the powers of and duties for these authorities in considerable detail and requires them to exercise such powers and duties "impartially, fairly and within a reasonable time."[178] Finally, the GDPR establishes a new European Data Protection Board, which is to coordinate actions among national commissioners and resolve disputes among them.[179]

B. CONTRACT AND CONSENT IN THE GDPR

In the EU, both contract and consent provide a legal basis for data processing. At the same time, the EU's collective approach to data privacy narrows these doctrines in a way that is unknown to American information privacy law. In the EU, contract is cabined by requirements of necessity, purpose limitation, and the ban on tying. As for consent, it is subject in the EU to strict requirements that make this doctrine unusable in many contexts of personal data processing.

1. Contract

In Article 6(b), the GDPR explicitly includes contractual agreements as a basis for lawful use of personal data.[180] It also provides significant limitations on this doctrine through requirements of "necessity" and the "purpose limitation." Its precise language permits processing of personal information when it is "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."[181] The key term here is "necessary." In the EU, all data processing requires a legal basis and is permissible only to the extent of those grounds. This restriction on the range of the contractual basis for processing is reinforced by the "purpose limitation." Under this principle, information cannot be "further

176. These state organizations must be "entirely free from instructions and pressure" to be able to carry out their tasks in "an objective and impartial manner." GDPR, *supra* note 8, at art. 52. The national supervisory authorities have constitutional rank in the EU, and as the European Court of Justice made clear in 2015 in its *Schrems* decision, the EU Commission lacks power to limit the scope of their powers. *See generally* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 91 (Oct. 6, 2015).

177. GDPR, *supra* note 8, at art. 52.

178. *Id*. at Recital 129.

179. *Id.* at ¶ 68.

180. *Id.* at art. 6.

181. *Id.*

processed in a manner incompatible with" the original purpose of collection.[182] Use of information beyond that which is necessary for the contract is impermissible.

The concepts of necessity and purpose limitation are longstanding EU restrictions on contract; they are found in the Directive and GDPR alike. To this mix, the GDPR adds a new ban on tying. The idea is that the terms within a single contractual agreement cannot be extended, or "tied," to include processing of personal data beyond that which is necessary to the purpose of the contract.[183] The ban on tying consolidates restrictions regarding necessity and purpose limitation; it also takes aim at myriad new digital business models based around data trade.

The critical concept is expressed in the GDPR's Article 7(b). It states that agreement to the "performance of a contract, including the provision of a service" is invalid if made "conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[184] In other words, a contract cannot tie consent for an initial data processing operation to a second one. In the assessment of Ulrich Dammann, the GDPR's ban on tying is "unique in the entire world."[185]

Finally, in evaluating the permissibility of contracts involving personal data, EU law draws on its consumer protection law. The GDPR requires a policing of the substantive terms of the contract as well as the form of its presentation. Concerning substance, the GDPR's Recital 42 references the Council Directive of 1993 on Unfair Terms in Consumer Contracts, which includes an expansive "black list" of unfair terms.[186] Its sweeping rule is that any contractual term which has not been individually negotiated is unfair if "it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."[187] The GDPR makes these protections part of the future DNA of EU privacy law. Concerning presentation, it requires that a contract contain information about the identity of the responsible data processor and "the purposes of the processing for which the personal data are intended."[188]

2. Consent

Long before the GDPR, EU data protection had established the current two-track approach to consent. The GDPR adopts this model, which is found in

---

182. Manfred Monreal, *Weiterverarbeitung nach einer Zweckänderung in der DS-GVO*, ZEITSCHRIFT FÜR DATENSCHUTZ 250, 252 (2016).

183. Ulrich Dammann, *Erfolge und Defizite der EU-Datenschutzgrundverordnung*, ZEITSCHRIFT FÜR DATENSCHUTZ 307, 311 (2016).

184. GDPR, *supra* note 8, at art. 7.

185. Dammann, *supra* note 183, at 311.

186. GDPR, *supra* note 8, at ¶ 42.

187. 1993 O.J. (L 95). *See* Jane K. Winn & Mark Webber, *The Impact of EU Unfair Contract Terms Law on U.S. Business-to-Consumer Internet Merchants*, 62 BUS. LAW. 209, 217 (2006) (analyzing the Unfair Terms Directive and its "non-exclusive list of terms that may be deemed unfair.").

188. GDPR, *supra* note 8, at Recital 42.

the Directive and national statutes, and further refines it. In the EU, consent is, first, a legal basis for data processing, and second, subject to significant restrictions that greatly narrow the permissible circumstances of recourse to it. Consent therefore proves a far less attractive ground for justifying the use of personal information than American lawyers may realize. To be sure, both the Directive and GDPR explicitly permit it as a basis for data processing. As GDPR Article 4(11) states, consent is a way to signify "agreement to the processing of personal data relating to him or her."[189] But consent is also subject to a host of limitations far beyond those that typically accompany this doctrine in U.S. law.

As an initial matter, the GDPR requires that consent be "freely given, specific, informed and unambiguous."[190] Thus, the GDPR disfavors the use of silence or inaction to constitute consent. Mechanisms for gathering consent must be understandable and transparent. As a further restriction, consent can be withdrawn at any time and, as noted above, it cannot be put into a contract for an unrelated matter.[191] Where consent involves the personal data of a child or sensitive data, there are additional enumerated conditions that must be met.[192] Finally, the burden of demonstrating consent is placed squarely on the data processor, who, in data protection terminology, is called "the controller."[193]

In sum, the GDPR reflects a restrictive view of consent, one that is stricter than the Directive. In his treatise on EU data protection law, Kuner advises organizations to seek paths other than consent to justify their processing of personal data.[194] He recommends that companies "reduce their reliance on consent as a legal basis for data processing to situations where it is absolutely necessary."[195] Kuner's recommendation from 2007 was based on his reading of the Directive and similar advice regarding a limited use of this doctrine is merited under the GDPR as well.

C. CONSTRUCTING A LEGAL IDENTITY THROUGH DATA PRIVACY

Rights talk forms an essential part of the European project, one that has become more central over time. As Fabbrini notes, there has been a "growth of

189. *Id.* at art. 11.

190. *Id.*

191. The strictest formulation of these requirements is expressed by the Article 29 Working Party in its 2011 Opinion on consent. This influential committee of data protection commissioners of member states developed a four-step test for gauging the validity of consent to data processing; each step must be fulfilled for consent to be legally valid. These requirements are that consent must be (1) a clear and unambiguous indication of wishes, (2) freely given, (3) specific, and (4) informed. Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 01197/11/EN (WP187) 35 (2011).

192. GDPR, *supra* note 8, at art. 8(1).

193. *Id.* at art. 12(5).

194. KUNER, *supra* note 173, at 68.

195. *Id.*

a fundamental rights culture in Europe in the last few decades."[196] Data protection law is at the front ranks of this effort. The EU began as an economic trading zone, but has always been about more than rationalizing a trade in coal and steel or safeguarding the free movement of goods. Constructed in the aftermath of the destruction of World War II, the European community rests on a desire for a new model of political cooperation with the goal of bringing lasting peace to Europe. Meeting this goal led to the creation of a supranational authority, one with "the power to bind its constituent member states."[197] Yet, the rise of these largely Brussels-based institutions has not been without challenges.

Of the considerable hurdles faced by the EU project, one of the most significant has been the "democratic deficit" of its institutions.[198] The ordinary European citizen feels bound to her national government, but is likely to have a more distant relationship with the EU as a sovereign entity. Too often, the EU is considered a distant, inaccessible institution. There are complaints about its transparency, complexity, the dominance of its executive institutions, the inability of its citizens to replace important decision-makers, and the lack of power for more democratic EU institutions.

One response has been to increase the power of the European Parliament. Starting in 1979, EU reforms have made it a directly elected body and assigned it more traditional kinds of legislative power. Nonetheless, as Paul Craig and Grainne de Búrca warn, "The problems of secrecy, impenetrability, accountability, and representativeness are not addressed simply by giving added powers to the European Parliament."[199] Another response to the democratic deficit in the EU has been made at the constitutional level.

The hope has been to create a sense of European citizenship through development and enforcement of European constitutional rights. Jürgen Habermas, the German philosopher, has emerged as one of the clearest voices for constitutionality as the key to Europe's future. In his analysis, the EU is made up of citizens of the member states ("We the People") as well as the nations of Europe.[200] Each individual therefore participates in the EU in a double fashion: both as a European citizen and through a role in her home nation.[201]

In turn, the EU must provide its citizens with constitutional guarantees of justice and freedom. Human dignity is the bedrock on which these guarantees rest. As the Charter of Fundamental Rights states in its Article 1: "Human dignity is inviolable. It must be respected and protected."[202] Above all, Haber-

196. FABBRINI, *supra* note 42, at 13.

197. PAUL CRAIG & GRAINNE DE BÚRCA, EU LAW: TEXTS, CASES, AND MATERIALS 5 (4th ed. 2008).

198. *Id.* at 58.

199. *Id.* at 133.

200. HABERMAS, *supra* note 19, at 66.

201. *Id.* at 70. For an analysis of the "strident and uncompromising" voice of Habermas on questions of European unity, see Jeremy Waldron, *The Vanishing Europe of Jürgen Habermas*, N.Y. REV. BOOKS 70 (Oct. 20, 2015).

202. Charter, *supra* note 39, at art. 1.

mas stresses the need for construction of a "common public sphere" in which citizens of Europe will engage in democratic deliberation.[203] Rather than as Croatians, Czechs, Frenchmen, or Italians, Europeans are to discuss issues that require transnational solutions in a new shared, deliberative space.

This new communicative area, Habermas's "common public sphere" for EU citizens, is far from established. But the EU is further along in development of a shared political identity based on common fundamental rights. The rights talk around data protection should be understood within this context. Here is the forward-looking focus of EU data protection; it seeks to create a constitutional basis for a pan-European identity. To be sure, there are other foundational elements for the EU's interest in privacy and data protection. The first element concerns integration of member states around a common market. As Abraham Newman argues, one goal of EU regulators has been to draw on their powers to further market integration.[204] Similarly, both the Directive and GDPR reflect, in part, such a market purpose.[205] Early caselaw of the European Court of Justice interpreting the Directive also emphasizes this "market integration objective."[206]

The second element is the continent's terrible experience of fascism, totalitarianism, and authoritarianism. The experience with the data gathering of different kinds of secret police in Western and Eastern Europe alike has profoundly heightened sensitivities towards data protection throughout the EU.[207] The rise of dignity and personality interests in European law after World War II played an important part in the later development of information privacy rights.[208]

To view EU data protection law, however, as resting only on the internal market and the lessons of the past, however crucial, would be to ignore its equally important role in the rights-oriented European project. Europe is no longer conversing in different languages when it comes to data protection law, but now speaks "European." The European language of data protection is now formed through the decisions of the European Court of Human Rights, the European Court of Justice, the GDPR, and a shared institutional structure, which includes the European Data Protection Board, the European Data Protection Supervisor, and national data protection authorities. Data protection is a critical part of the EU's development of European human rights law. In this regard, Fabbrini points to a 2014 decision of the European Court of Justice invalidating the EU's Data Retention Directive as the ruling that "crowns a

---

203. HABERMAS, *supra* note 19, at 59–61.

204. ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY 75 (2008).

205. ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 8 (2015).

206. *Id.* at 51–54.

207. On the rise of dignity and personality interests after the horrors of World War II, see Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's* Privacy *and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CAL. L. REV. 1925, 1948–49 (2010). For a differing account of these developments, see James Q. Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1180–89 (2004).

208. For an introduction to the German constitutional case law in this area, see KOMMERS, *supra* note 57, at 298–359.

decade of progressive jurisprudential developments in the field of human rights."[209]

III. THE UNITED STATES: PROTECTING THE PRIVACY CONSUMER

U.S. privacy law situates the consumer within a marketplace for data trade. In it, the FTC has a central role through its policing data exchanges against the most deceptive kinds of practices. There is considerable distance here from the EU's rights discourse about data subjects. There are equally important differences between the United States and EU regarding the comparative constitutional aspects of information privacy law and data protection law, and the incorporation of doctrines of contract and consent.

This Part demonstrates that the United States makes scant use of consent and contract. Its privacy statutes rely on forced disclosure by data processors of information about their practices and obligatory receipt of this information by privacy consumers. Moreover, the FTC creates a legal fiction around "consent" of a privacy consumer to police the privacy marketplace. This Part concludes by exploring the minor reliance on formal doctrines of consent and contract in U.S. information privacy law and the resulting favorable landscape for data processors.

A. POLICING THE MARKETPLACE: STATUTES AND THE FTC

In contrast to the EU, U.S. law does not rely heavily on information privacy inalienabilities. To be sure, its patchwork of sectoral law does impose certain affirmative obligations on companies that must be followed. Notwithstanding that point, and as a first distinction with the EU, U.S. information privacy does not establish an essential set of nonwaivable requirements for "lawfulness of processing," as Article 6 of the GDPR does.[210] The second difference is that it does not place strong restrictions on consent and contract.

At the statutory level, the most important inalienabilities concern mandated disclosure and notice regarding privacy practices.[211] In the United States, the FTC makes the most important use of a privacy inalienability. It does so through its "notice-and-consent" enforcement approach. The FTC proceeds through enforcement of the wishes of a reasonable consumer and the idea that this individual has agreed only to certain data practices.

---

209. Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65, 81 (2015). The 2014 case that Fabbrini points to as a turning point has been expanded by a subsequent 2016 data retention decision of the same court, Tele2 Sverige AB v. Post- och telestyreisen, ECLI:EU:C:2016:970 (Dec. 21, 2016) (Data Retention).

210. GDPR, *supra* note 8, at art. 6.

211. *See, e.g.*, The Gramm–Leach–Bliley Act, 15 U.S.C. § 6803 (1999) (requiring financial institutions to provide consumers with notification of their companies' privacy practices); California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014) (requiring commercial websites that collect personal information from visitors to post their policy practices).

1. Statutes

In the United States, statutes create information privacy inalienabilities by imposing disclosure requirements on companies. These mandated disclosures bolster the FTC's existing "notice and consent" approach; the statutes in question require certain companies to spell out their data processing practices. This "turn to disclosure" also occurs in many other areas of law. In a comprehensive study of these practices, Omri Ben-Shahar and Carl Schneider observe, "[D]isclosures were mandated almost wherever we looked."[212] In their finding: "There [are] hundreds of statutes, regulations, and rulings mandating countless disclosures, all trying to do the same thing: give lay people information to help them make better decisions as consumers, cardholders, patients, employees, tenants, policyholders, travelers, and citizens."[213]

U.S. privacy law relies on forced disclosure for data processors and forced receipt of the information by privacy consumers. It removes such information about data exchanges from the realm of negotiations between merchants and individuals. Numerous U.S. privacy laws and regulations—both federal and state—require that individuals receive information about how organizations plan to use their personal information.[214] The GLBA is a leading example of such a federal law; it requires financial institutions to supply consumers with notices that explain these companies' privacy practices.[215] As the FTC summarizes, "The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information."[216]

Another area of mandated disclosure concerns data breach notifications, which are required by forty-eight states and for covered health care information by the federal HITECH Act.[217] State law has also imposed notification requirements beyond data breach notification. In California, for example, all commer-

212. OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE, at ix (2014).

213. *Id.*

214. *See, e.g.*, Gramm–Leach–Bliley Act, 15 U.S.C. § 6803 (2012) (requiring financial institutions to provide consumers with notification of their companies' privacy practices); Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 300jj–300jj-52 (2012) (requiring mandated disclosure of breaches of covered health care information). There are also now 48 states with mandated data breach notifications. For a list of 47 of these states, see DANIEL SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 205–07 (2017). On April 6, 2017, New Mexico became the 48th state to enact a data breach notification law. Data Breach Notification Act (H.B. 15).

215. 15 U.S.C. § 6803.

216. FTC, IN BRIEF: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM–LEACH–BLILEY ACT (July 2002), https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act [https://perma.cc/XMY8-TNKE].

217. For a summary chart of the state data breach notification statutes, see SOLOVE & SCHWARTZ, *supra* note 214, at 207–09. For HITECH data breach notification requirements, see HEALTH & HUMAN SERVS., HITECH BREACH NOTIFICATION INTERIM FINAL RULE, https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/HITECH/index.html.

cial websites must post a privacy policy if they collect personal information from their visitors.[218] California also requires financial privacy disclosures with slightly different content than that under the GLBA; consequently, Californians receive two types of notices, with almost complete overlap, from their financial institutions.[219]

Such disclosure requirements are mandatory and cannot be waived by individuals. Many consumers, buried under an avalanche of privacy notices, might yearn to stop the flow of paper and the slaughter of trees. In noting the widespread use of such mandates, Ben-Shahar and Schneider sum up their view of the impact of the resulting information burdens: "Disclosure is a ritual to be endured."[220]

2. Idealized Consent

In the United States, the FTC draws on Section 5 of its organic act, as amended in 1938, to police the privacy marketplace. The result has been privacy protections for consumers that are untethered to the boundaries of sectoral statutes. There are, nonetheless, restrictions on the FTC's jurisdiction.

First, it is limited to industries that fall under the FTC's organic act.[221] Second, and as a more pervasive restriction, this agency can act under Section 5 only to prevent "unfair or deceptive acts or practices in or affecting commerce."[222] Despite these restrictions, the FTC has acted creatively in drawing on an idealized conception of consumer consent in its actions. It starts with the premise that a reasonable consumer has an expectation regarding certain data practices, whether explicitly promised or more reasonably to be expected from that kind of company in that sector. The privacy consumer then consents to sharing data based on this explicit or implicit understanding, and the FTC then enforces a company's failure in this regard as unfairness or deception.

In its enforcement actions in the informational privacy context, moreover, the FTC has favored using its authority against deception. A deceptive act or practice, in the FTC's longstanding definition, is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[223] The core group of the FTC's deceptive enforcement actions rests on its theory of notice-and-consent.[224]

---

218. California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014).

219. For more details regarding the requirements under the California Online Privacy Protection Act, see LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW 179–81 (2d ed., 2017).

220. SHAHAR & SCHNEIDER, *supra* note 212, at 10.

221. 15 U.S.C. § 46 (2012). For a discussion of these jurisdictional requirements in the privacy context, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 602–04 (2014).

222. 15 U.S.C. § 45 (2012).

223. FTC Policy Statement on Deception, 103 F.T.C. 174 (1983).

224. For an evaluation of the FTC's notice-and-consent jurisprudence, see HOOFNAGLE, *supra* note 123, at 365; Solove & Hartzog, *supra* note 221, at 636–38.

The FTC's notice-and-consent enforcement considers an organization's privacy statement to supply "notice" and a consumer's subsequent sharing of personal information with that entity to manifest her "consent" to the data practices covered under that statement. The FTC then seizes on the merchant's failure to follow its stated practices or a reasonable consumer's expectations as proof of deception in the marketplace. This agency has engaged in numerous enforcement actions under this rubric and collected millions of dollars in fines in settlements.[225] The FTC has even read a limited number of substantive requirements into its deception jurisprudence. As Daniel Solove and Woody Hartzog summarize, deception in the FTC's view can be by omission of relevant information, insufficient notice, or even through a clearly objectionable practice, such as "pretexting."[226]

In the uncertain privacy landscape of the United States, the FTC has stopped companies from tricking consumers, overpromising privacy, and engaging in unexpected and unreasonable data practices. Yet, this agency's connection between deception and consent rests on an idealized view of consumer consent—that is, on a "legal fiction." In the definition of Lon Fuller, a legal fiction involves the reconciliation of "a legal result with some expressed or assumed premise."[227] The FTC's assumed premise is that an imagined reasonable consumer read a privacy statement and agreed to the terms in it as well as other aspects of a consumer's impressions of the company's privacy representations. These other aspects might include the blog posts of an executive, a consumer-facing computer interface, or aspects of a product's design.[228]

The deceptive merchant, then, flouted this reasonable individual's consent. In reality, most consumers do not read privacy policies and are unaware of company's data policies. To put the resulting situation into aphoristic terms, we can state, "No one has ever read a privacy notice who wasn't paid to do so." More generally, the FTC assumes that a consumer had settled expectations of reasonable merchant practices—even regarding technology that might be unknown to the consumer.

As is true for some other legal fictions, however, there are benefits to the FTC's notice-and-consent framework. It allows this agency to police the personal data marketplace. And the FTC does so by a collective enforcement strategy of the type that EU data protection law carries out on a far greater scale. In stopping such unfair or deceptive commercial behavior, the FTC acts against practices that precede consensual agreement and are independent of contractualism.

---

225. *See, e.g.*, *In re* Sears Holdings Mgmt. Corp., 2009 WL 2979770 (Aug. 31, 2009).

226. Solove & Hartzog, *supra* note 221, at 628–38. As for unfairness, the FTC developed the second prong of its privacy jurisprudence subsequent to its deception enforcement and has taken fewer actions based on it. For an explanation of the considerable limits on unfairness as a tool for enforcing privacy, see HOOFNAGLE, *supra* note 123, at 160.

227. LON L. FULLER, LEGAL FICTIONS 51 (1967).

228. HOOFNAGLE, *supra* note 123, at 145.

B. CONTRACT AND CONSENT IN THE PRIVACY MARKETPLACE

Based on the American legal system's general openness towards contractual ordering, one might expect heavy recourse in information privacy law to this legal mechanism. The U.S. approach to contracts is favorable to letting parties reach agreement on their own terms.[229] Yet contract proves largely irrelevant to information privacy law in the United States. There are relatively few cases involving this doctrine, and these show a divide between courts that view privacy notices as possible contracts and those that see them only as nonbinding expressions of preferences. Either interpretation leads to a notable lack of protection for consumers. For data processors, the news is all good: for them, contract is a realm of "heads, I win; tails, you lose." As for consent, U.S. law makes minor use of it.

1. Contract

U.S. law lacks a requirement of a legal justification for personal data processing; therefore, data processors can collect and use personal data without contract. Their only requirement is to follow any sectoral laws or other legal requirements that may exist.

Where the issue of contracts has arisen, it is because of the "turn to disclosure" in information privacy law. As noted above, American law encourages and, in some instances, requires data processors to reveal their information practices. Now commonplace, privacy policies typically explain the categories of personal data that the company collects, the kinds of parties with whom this information is shared, and the interests, if any, that the document provides an individual in her information, including rights of access and correction. The issue then becomes whether such privacy policies or notices constitute a contract. Some courts have held that these statements are per se unenforceable in contract; other courts have held that they might be contracts, but then tend to rule plaintiffs cannot recover for other reasons, such as lack of damages.

As for courts that are contract skeptics, these judges consider a company's privacy policy to be nonbinding statements of policy. As an example, plaintiffs in a class action lawsuit alleged in 2005 that Northwest Airlines violated a contractual promise that information it collected would be used only for limited purposes.[230] The airline had, in fact, shared extensive consumer data with a federal agency to assist in its study of airline security.[231] For the *Northwest* court, however, the airline's promises were only "general statements of policy."[232] It concluded that the privacy notice posted on the airline's website did not

229. As Robert Braucher—then Professor of Law at Harvard Law School and soon to be a justice on the Massachusetts Supreme Court—put it, "Freedom of contract, refined and redefined in response to social change, has power as it always had." Robert Braucher, *Freedom of Contract and the Second Restatement*, 78 YALE L.J. 598, 616 (1969).

230. *See In re* Nw. Airlines Privacy Litig., 2004 WL 1278459, at *5 (D. Minn. June 6, 2004).

231. *Id.* at *5.

232. *Id.* at *6 (quoting Martins v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 741 (Minn. 2000)).

constitute a contractual agreement with the company's customers.[233]

As for the second group of courts, some judges have been willing to decide, at least in the context of a motion for summary judgment, that a company's policy might be considered a contract. The leading cases in this camp are *In re JetBlue Airways Corp. Privacy Litigation*[234] and *In re American Airlines Inc. Privacy Litigation*.[235] Notably, both cases still led to resounding victories for the corporate defendants. Even if a privacy policy might be the basis for a contract, these courts found that the plaintiffs failed to provide sufficient proof of contractual damages to survive the motions for summary judgment. When a company fails to uphold its part of the contractual bargain, black-letter law holds that an action for breach can proceed only where the plaintiff incurs damages. For various reasons, these courts have held that a company's use of information beyond that of the contract does not harm the plaintiff.[236] The Restatement of Consumer Contracts, now in the drafting process, contains a thorough survey of the current caselaw and finds "[w]hile it is not uncommon for courts to dismiss breach-of-contract claims for privacy-notice violations," the leading cause of such dismissal proves to be, as in the airline cases above, "failure to ascertain damages for breach of contract."[237] No harm, no foul, and no violation of any contract that might exist.

In sum, the bottom line is likely to be the same whether the future leads to courts reading privacy policies as contracts.[238] Contract law in the United States will play a modest role in information privacy law and do little to protect privacy consumers.

2. Consent

In the United States, unlike the EU, there is no need to gain an individual's consent for data processing, and, hence, data processors are not generally obligated to rely on a consensual mechanism. Statutory law in the United States does make use of consent, however, in two variants. These are "opt-in" and "opt-out" consent. Under opt-in, a processing of personal data cannot take place unless the individual gives her affirmative permission. Under opt-out, data processing takes place unless the individual objects. In a limited fashion, U.S.

---

233. 2004 WL 1278459, at *6.

234. 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

235. 370 F. Supp. 2d 552, 554 (N.D. Tex. 2005).

236. As the district court in *In re Jet Blue Airways Corp. Privacy Litigation* concluded, "There is . . . no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large." 379 F. Supp. 2d at 327. Because personal information is, according to this court, not freely tradeable, an alleged misappropriation of it in violation of contract did not harm anyone. *Id.*

237. ALI, Restatement of the Law, Consumer Contracts, Council Draft No. 3 13–14 (Dec. 20, 2016). The second major cause is "failure of consideration or lack of mutuality." *Id.*

238. Of the two camps regarding privacy-policies-as-contracts, the Draft Restatement of Consumer Contracts identifies a trend toward courts holding that "privacy notices could give rise to contractual obligations." *Id.* at 15.

law uses opt-in to fulfill a "warning function" on behalf of the privacy consumer. Overall, both kinds of consent play a secondary role in U.S. information privacy law.

a. Opt-in. The FCRA contains one of the strongest opt-in mechanisms for consent in U.S. information privacy law. The first federal information privacy law in the United States, the FCRA regulates use of "consumer credit reports" by "consumer reporting agencies."[239] A credit reporting company can widely share credit reports for a broad set of purposes, including when it has "reason to believe" that there is "a legitimate business need for the information."[240] These permissible transfers of data and resulting use by the recipient third party occur without the affected consumer's consent.

The FCRA turns to consent mechanisms, however, when consumer credit reports are to be used for employment purposes,[241] or when they contain medical information.[242] Congress in amendments to the FCRA in 1996 viewed these areas as more sensitive than others in which credit reports were used.[243] Therefore, it sought to involve the consumer by informing her of the planned use and requiring her consent.[244] Congress uses opt-in consent in this statute as a limited warning mechanism. It is intended to trigger consumer attention to the moment of data exchange. Before an employer or potential employer can use a consumer report for employment purposes, she must provide the affected person with "clear and conspicuous disclosure" of the planned use of the report and obtain "written authorization" from the consumer.[245] Consent requirements are further heightened should there be a planned use of medical information, whether for purposes of employment, or for credit or insurance transactions.[246]

The statute does not, however, concern itself with the possibility of power imbalances in the employment or other relationships. Thus, the individual may lack any real ability to deny a potential employer access to her credit record—at least if she wants the job in question. The FCRA also ignores the extent to which consumers are overwhelmed by life's daily information demands, whether or not opt-in is required. Ben-Shahar and Schneider term this issue, "the accumulation problem."[247] As they note, "A single disclosure may be manage-

239. For a history of the FCRA, see SOLOVE & SCHWARTZ, *supra* note 30, at 743–44; Kristen J. Matthews, *Financial Privacy Law § 2:2.1*, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE (2d ed. 2017)

240. 15 U.S.C. § 1681b(a)(3)(F) (2012).

241. *Id.* § 1681b(b).

242. *Id.* § 1681b(g).

243. Omnibus Consolidated Appropriations Act of 1997, P.L. 104–08, The Statute at Large, at 110 Stat. 3009-430 (1997).

244. 15 U.S.C. § 1681b(b)–(g).

245. *Id.* § 1681b(b). The employer must also certify to the consumer reporting agency that it has obtained this consent and that it will not use the information in violation of applicable equal employment opportunity law. *Id.*

246. *Id.* § 1681b(g).

247. SHAHAR & SCHNEIDER, *supra* note 212, at 95.

able, but en masse, disclosures are overwhelming, and people cannot hope to attend to more than a trickle of the flood."[248]

Another use of opt-in consent is found in the VPPA.[249] Yet this statutory requirement's impact on consumer privacy is highly limited. The "warning function" of consent in the VPPA regards the sharing of "prerecorded video content," but its scope is restricted to information about the title and content of audio-visual material. The VPPA permits release of other information about the customer's relationship with the video-providing company.

b. Opt-out. Under opt-out consent, an entity may use personal information unless the affected individual objects. If the individual takes no action, the personal data use occurs. The GLBA illustrates how ineffective this right of refusal typically proves. Congress enacted the GLBA for purposes other than information privacy; most of the Act serves to repeal the Depression-era Glass–Steagall Act to permit the creation of large financial "supermarkets" in the United States. At the same time, Congress anticipated that these new financial entities would have access to large amounts of information about consumers. In Title V of the GLBA, it set rules for these companies' use of personal information.[250] The GLBA's general approach is to permit use of such information, but to require its regulated entities to provide data security and ample notice of their data practices to consumers. Financial institutions can use personal information without consumer consent inside their corporate structure and even with "affiliated entities" outside of it.

Consumer consent only comes into play under the GLBA regarding a small subset of data use. It occurs when a financial institution seeks to share information with an entity external to its corporate universe. The term of art in the GLBA to describe such an outside organization is the "nonaffiliated third party."[251] When a financial institution reaches beyond its own corporate structure or affiliated parties to share data with such an entity, the GLBA requires an opt-out. A consumer "is to be given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party."[252] In a critique of this practice in 2002, one of the coauthors of this Article observed that the GLBA "leaves the burden on bargaining on the less informed party, the individual consumer."[253]

Finally, even if a consumer opts out of GLBA, a joint marketing exception allows some sharing of personal information.[254] For example, a financial institu-

248. *Id.*
249. 18 U.S.C. § 2710 (2012).
250. 15 U.S.C. §§ 6801–6809 (2012).
251. *Id.* § 6802.
252. *Id*.
253. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1241 (2002).
254. Privacy of Consumer Financial Information, 16 C.F.R. § 313.13(b) (2017).

tion can transfer personal information to a nonaffiliated company to sell jointly offered services or products.[255] A co-branded credit card would be this kind of jointly marketed product.[256]

In sum, opt-out consent in the United States has not effectively protected consumer privacy rights. For Daniel Solove, the blend of notice-and-consent mechanisms represents the flawed practice of "privacy self-management."[257] Solove warns of considerable "structural problems" that involve "impediments to one's ability to adequately assess the costs and benefits of consenting to various forms of collection, use, and disclosure of personal data."[258] U.S. data privacy law views the consumers, however, as innately sovereign.

C. CONSTRUCTING LEGAL IDENTITY THROUGH DATA PRIVACY

How is one then to understand the U.S. approach? One should begin by noting the weak constitutional status of information privacy in the United States. An approach in the United States based around rights talk would therefore be unlikely to gain traction. The U.S. Constitution is one of "negative rights" and has scant reach into private sector activities.[259] Existing constitutional protections, such as the Fourth Amendment and Fourteenth Amendment, prove a poor fit with the Information Age's development of governmental databases and widespread sharing of data by individuals with "third parties." If anything, the U.S. Constitution serves as a force for strengthening the rights of data processors.

For the United States, the idea of the privacy consumer is far more promising than a "rights model" for privacy because it ties into deep-rooted ideas. As James Whitman perceptively observes, "The key identity for Americans, is, as so often, the consumer sovereign."[260] Americans trust in a notion of progress tied to technology and "innovation." The last word is especially cherished by tech gurus in Silicon Valley and policymakers in Washington, D.C.[261] From the start of the Internet's commercialization, it has been associated with benefits to consumers as well as the creation of great wealth for the U.S. economy. As

255. *See* Privacy of Consumer Financial Information, 16 C.F.R. § 313.13(a)–(b) (2017) (noting that opt out requirements do not apply when a company provides personal information to a nonaffiliated third party to market financial products or services offered pursuant to joint agreements between a company and a financial institution).

256. *See id.* § 313.13(c) (defining a joint agreement as "a written contract pursuant to which you and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service").

257. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013).

258. *Id.* at 1888.

259. As discussed *supra*, a positive right requires the state to take certain actions, and a negative right requires it to refrain from certain actions. On the broad reach of European constitutional rights, see generally SWEET, *supra* note 40.

260. Whitman, *supra* note 29, at 399.

261. Indeed, in Dave Eggers' novel, *The Circle*, the word "innovate" appears emblazoned on a stone in a walkway of the Internet company that rules this novel's dystopian world. DAVID EGGERS, THE CIRCLE 2 (2013).

Thomas P. Hughes, a historian of technology, notes, "Technology linked to mass consumption is a modern American hallmark."[262]

In a reflection of these background values, U.S. information privacy law has embraced marketplace discourse and protected the privacy consumer. Congress and the FTC provide proof of this concept. When they have enacted privacy legislation, federal lawmakers have done so to protect consumers within different information marketplaces. Beyond that, they are unwilling to legislate—as demonstrated by the rejection of omnibus privacy legislation as early as 1974.[263] The FTC has acted to stop deceptive trade practices and, to a lesser extent, unfairness in the marketplace.[264] But its notion of deception and unfairness ultimately rest on a notion of consumer detriment, which narrows its vision to market relations.

IV. DATA PRIVACY'S INTERNATIONAL FUTURE

We have now assessed the basis for each legal system's reliance on either rights talk or marketplace discourse. This analysis also illuminates the differing role of contract and consent in each system. The EU must necessarily turn to contract and consent because it requires a basis in law for personal data processing. As an expression of individual self-determination, consensual mechanisms traditionally occupy a pride of place. At the same time, data protection law limits contract and consent because of the unfortunate results of unbridled reliance on them. In the real world, data subjects face numerous hurdles in exercising sovereign choice. The real world is one of power imbalances and bounded rationality. In anticipation of bad results through borderless consent and contract, EU data protection law channels and restricts these doctrines. In the United States, in contrast, consumers are free to act in a marketplace for data trade and to take advantage of a dazzling array of services and products built around the free flow of information. The legal system acts to stop the most blatant failures of the data marketplace. It does so by policing against deception and unfairness and in promoting mechanisms of notice and disclosure. Consent and contract by the individual play a scant role within the U.S. system for information privacy.

Thus, this Article has identified a conceptual gulf between the data privacy systems of the EU and United States based on the different legal identities that they provide for the individual. In turn, these different approaches are significant for the "transatlantic data war" concerning data transfers. There is also deep skepticism at present on each side towards the other.

---

262. THOMAS P. HUGHES, AMERICAN GENESIS: A CENTURY OF INNOVATION AND TECHNOLOGICAL ENTHUSIAM 1870–1970, at 471 (1989).

263. For a discussion of this path not taken, see REGAN, *supra* note 133, at 77–79.

264. On the FTC's preference for the deception prong of the FTC Act over unfairness, see HOOFNAGLE, *supra* note 123, at 132–40.

In the United States, some consider EU data protection as a form of trade protectionism, or the result of misguided jealousy toward successful U.S. Internet companies. Here is how President Barack Obama analyzed European investigations into Facebook and Google: "[O]ftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."[265] There is also a feeling in the United States that its approach is far more promotive of innovation than EU data protection, seen as having stifling rules for tech firms. Thomas Davenport went a step further in arguing that Congress was not to be trusted to craft privacy legislation. He noted, "If they can't pass a budget or a debt-ceiling increase, they have no business venturing into complex online privacy issues."[266] In his judgment, the most likely outcome from Washington would be "a bad law."[267]

Similar doubts exist on the EU side regarding American privacy. Jan Albrecht, the EU Parliament's rapporteur for the GDPR, explains: "In the USA, the handling of our personal information is governed solely by the very vague rules of fair competition and by considerations regarding the image of the company that will be created amongst consumers themselves."[268] In assessing U.S. information privacy, Andreas Börding calls attention to its "structural deficits."[269] The former data protection commissioner of a German state, Schleswig-Holstein, Thilo Weichert argues that U.S. companies rely on a "Violation-of-Data-Protection Business Model."[270] The stagnation of U.S. privacy law has made this model possible. In particular, Weichert contends that the understanding of fundamental rights for the digital age in U.S. privacy law has failed to advance beyond the 1970s.[271] More broadly, EU policymakers view fundamental data protection rights as something that cannot be left to the market.

Thus, policymakers and academics in each system view the other side with doubt and sometimes disbelief. Finding a way forward will be greatly assisted by understanding the deeper grounds for differences in the systems. Parts A and B examine the question of transatlantic data flows. These parts discuss the demise of the Safe Harbor and assess the Privacy Shield in light of this Article's models of rights talk and marketplace discourse. Part C identifies elements for

---

265. Kara Swisher, *White House. Red Chair. Obama Meets Swisher*, RE/CODE (Feb. 15, 2015), http://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher [https://perma.cc/A5UX-XEES]. President Obama was speaking of EU antitrust investigations of Facebook and Google, but his comments are equally illustrative of U.S. attitudes towards their privacy activities regarding leading U.S. tech companies.

266. Thomas Davenport, *Should the U.S. Adopt European-Style Data-Privacy Protections?*, WALL ST. J. (Mar. 10, 2013), https://www.wsj.com/articles/SB10001424127887324338604578328393797127094 [https://perma.cc/W7GU-UW8Z].

267. *Id.*

268. JAN PHILIPP ALBRECHT, HANDS OFF OUR DATA! 47 (2015).

269. Andreas Börding, *Ein neues Datenschutzschild für Europa*, Computer und Recht 431, 434 (2016).

270. Thilo Weichert, Datenschutzverstoβ als Geschäftsmodell—der Fall Facebook, Datenschutz und Datensicherheit 716 (10/2012).

271. Thilo Weichert, Globaler Kampf um digitale Grundrechte, 47 Kritische Justiz 124, 127 (2014).

future convergence or divergence for international data privacy law. Finally, the Article examines the varied design choices in the GDPR and Privacy Shield and the resulting forces generated to shape behavior in both the EU and United States and create a new international law of data privacy.

A. INTERNATIONAL DATA TRANSFERS: THE ROAD TO THE SAFE HARBOR AND ITS DEMISE

This Article began by referencing the international conflict around transfers of personal data from the EU to the United States. We now discuss this topic in more depth. In this section, we trace the path to the European Court of Justice's invalidation of the Safe Harbor, which was the most important first-generation solution to the issue of international data transfers. This section describes the policy imperatives that led to the creation of the Safe Harbor and considers the grounds for its downfall.

By the late 1980s, European policymakers realized that their efforts to create strong safeguards for data protection necessitated transborder policies for the data of EU citizens. Because of global data flows, already present in that pre-Internet age, legal regulatory efforts in the EU were doomed to failure if their reach ended at the territorial borders of Europe.[272] From the EU perspective, permitting an abuse of European citizens' personal information *outside* of Europe would make a mockery out of the decades of work to create high levels of privacy *inside* Europe. Important efforts followed at the trans-European level and within member states to fashion a legal response to the perceived threat to privacy of international data transfers.

The resulting EU policy requirement then and now is an "adequate level of protection" in any non-EU recipient nation before an EU member state can transfer personal data outside of the EU. Both the Directive (1995) and the GDPR (2016) contain this "adequacy" requirement.[273] In consequence, data transfers from the EU to the United States have a questionable legal status. This legal uncertainty follows from EU skepticism about the sufficiency of U.S. information privacy law. In 1999, the Article 29 Working Party, the influential group of national data protection commissioners, summed up the European view of the matter. It declared that the "current patchwork of narrowly focused sectoral laws and voluntary self-regulation in the United States is not adequate."[274] Yet, with so much valuable data trade between the EU and United States, both sides had considerable incentives to find policy solutions to bridge their different legal approaches to data privacy. The most significant outcome of this policy effort was the Safe Harbor Agreement, a treaty negotiated by the U.S. Department of Commerce and the Commission of the EU.

The Safe Harbor represented a bold policy innovation: it transplanted EU data protection concepts into U.S. law in a fashion beyond the willingness of

272. For a discussion, see Schwartz, *supra* note 6, at 472.
273. DP Directive, *supra* note 7, at art. 56; GDPR, *supra* note 8, at art. 45.
274. Article 29 Working Party, *supra* note 10, at 2.

Congress or the ability of the FTC and other regulatory agencies. Its principles were intended to be close enough to those of EU data protection so that the U.S. companies in following them would provide "adequate" data protection. Although U.S. companies needed only apply the Safe Harbor Principles to the personal data of Europeans, they were also free to bring all their data systems into compliance with it and apply these standards to U.S. citizens. In some instances, U.S. organizations decided to do so for reasons varying from managerial simplicity to policy leadership.[275] In turn, the transplantation by the Safe Harbor of EU data protection onto U.S. territory proved politically palatable because decisions by U.S. companies to qualify for it were voluntary.

Another factor made the Safe Harbor acceptable in the United States. The Safe Harbor's negotiated standards weakened classic EU principles just enough to make the agreement tolerable on the American side of the Atlantic, but not too much to make them indefensible in Brussels. At least, the EU at first did not view these standards as excessively watered down.[276]

Despite grumblings in the EU about the Safe Harbor, this treaty's future success seemed assured for the twenty-first century with over 5,000 U.S. companies entering it.[277] When the Commission and the Commerce Department began to consider improvements in a "Safe Harbor 2.0" in 2012, many in the United States expected only tinkering with the accepted formula.[278] This expectation was, in turn, dashed by the Snowden revelations, which detailed widespread collaboration by American companies with the NSA and called into doubt the "adequacy" of the protection in the United States. Then on October 6, 2015, the European Court of Justice's opinion in *Schrems v. Data Protection*

---

275. *See, e.g.*, KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 65 (2015) (discussing interviews with U.S. corporate privacy officials that showed how some companies default "to the highest common denominator, which . . . is Europe").

276. Over time, the unhappiness at the EU with the Safe Harbor would grow. For an indication of this evolving attitude see its commissioned reports from Galexia—an Australia consulting company—on the framework's weaknesses, Chris Connolly, *EU/US Safe Harbor—Effectiveness of the Framework in relation to National Security Surveillance*, GALEXIA (Oct 7, 2013), http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf [https://perma.cc/BAX6-PUUZ] (testimony before the EU Parliament summarizing the 2008 and 2010 Galexia studies). For an analysis of the Galexia studies' strengths and weaknesses and further reflections on the "Unsafe Harbor," see THORSTEN HENNRICH, CLOUD COMPUTING 180–86 (2016).

277. The Department of Commerce continues to maintain the Safe Harbor List with its 5,457 entries. *See* U.S.–EU Safe Harbor List, EXPORT, https://safeharbor.export.gov/list.aspx (last visited Jan. 30, 2017). As for the grumblings in the EU, the Article 29 Working Party, made up of data protection commissioners, kept raising questions about the validity of the Safe Harbor until the moment of its invalidation. For an early example of this skepticism, see Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 7/99, 5146/99/EN/final, WP 27 (Dec. 3, 1999), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp27_en.pdf [https://perma.cc/5LLU-8658].

278. Regarding the discussion for a Safe Harbor 2.0, see the Commission's pre-Snowden recommendations. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspectives of EU Citizens and Companies Established in the EU, at 9, COM (2013) 847 final (Nov. 27, 2013).

Commissioner ended any hope of only minor changes to the Safe Harbor.[279] This judgment voided the Safe Harbor agreement and, thereby, immeasurably strengthened the hand of EU negotiators.

For the European Court of Justice, the *Schrems* case implicated its central role protecting fundamental rights. Maximilian Schrems was an Austrian national who used Facebook and objected to its transfer of his personal data from its servers in the EU to its servers in the United States. For Schrems, this activity violated the EU standard of "adequate" data protection because of "the activities of the United States intelligence services, in particular those of the National Security Agency."[280]

Regarding Snowden's leaks, the Luxembourg Court made clear its constitutional objections to the NSA activities.[281] In its opinion, it singled out for especially strong criticism the NSA's massive suspicionless data dragnets and bulk storage of information.[282] It identified a violation of Article 7 of the Charter by the Safe Harbor's providing access to the U.S. government of the data of EU citizens.[283] In *Schrems*, the Luxembourg Court also observed that "an adequate level of protection" in any international data transfer meant "a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the EU."[284] The *Schrems* decision marked a decisive caesura in EU–U.S. relations; it showed the EU judiciary to be willing to invalidate the leading mechanism for transatlantic data flow and to establish constitutional requirements for this activity.

B. THE PRIVACY SHIELD

In the aftermath of *Schrems*, the ongoing negotiations between the Commission and U.S. Department of Commerce took on new urgency. "Safe Harbor 2.0" was a brand without a future. In its place, the two sides reached an agreement on a new treaty, which they called the "EU–U.S. Privacy Shield."[285] The agreement took effect on August 1, 2016. Legal challenges have already been lodged against it, and, as for the Safe Harbor, the European Court of Justice will be the ultimate arbiter of the constitutionality of the Privacy

279. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 91 (Oct. 6, 2015).

280. *Id.* at ¶ 28.

281. *Id.* at ¶ 28.

282. *Id.* at ¶ 93.

283. *Id.* at ¶ 93. The European Court of Justice stated, "In particular, legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter." *Id.*

284. *Id.* at ¶ 73 (emphasis added).

285. *Remarks by U.S. Secretary of Commerce Penny Pritzker at EU–U.S. Privacy Shield Framework Press Conference*, U.S. DEP'T OF COM. (July 12, 2016), https://www.commerce.gov/news/secretary-speeches/2016/07/remarks-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield [https://perma.cc/XA93-BNCY] [hereinafter *Remarks*].

Shield.[286]

1. Negotiating Perspectives and Positions

This Article now revisits its respective models of EU and U.S. data privacy. Recall Gertz's concept of law as a form of social imagination.[287] Based on the two discourses about privacy, the EU and United States would necessarily view these negotiations from different vantage points.

From the EU perspective, there was a need to protect individuals from the state and private data processors alike. The language of rights also creates a strong connection between EU institutions and data subjects. These rights are protected as part of the data subject's identity as an EU citizen. Beyond these doctrinal touchstones, the EU came away from the Safe Harbor with a sense of disappointment about U.S. industry's compliance. As the *Schrems* decision noted, "a significant number of certified companies did not comply or did not comply fully, with the safe harbor principles."[288]

As for the view from the United States, the downfall of the Safe Harbor increased the need for a new agreement to permit free information flow with the EU. With its strong market orientation, the United States approached the negotiations favoring open choice for consumers regarding data use and broad access to innovative American data services and products.[289] Mechanisms around notice would fit in well with this system.

With these points in mind, we can now evaluate the Privacy Shield. Like the Safe Harbor, the Privacy Shield is best understood as a mixture of EU and U.S. standards. Post-Snowden and *Schrems*, the EU could tug the resulting agreement closer to its fundamental principles. At the same time, the United States could sign it because it contained weaker versions of some of the core EU principles of data privacy. Moreover, many elements of the framework depend on future decisions after initial deployment of oversight mechanisms. Hence, U.S. negotiators could in good conscience agree to it and trust in future collaborative decision making with the EU. The four core Privacy Shield Principles concern "data integrity and purpose limitation," "choice," enforcement, and oversight.[290] In assessing the Privacy Shield, we concentrate on those principles.

2. Data Integrity and Choice

The first key standard of the Privacy Shield is the "Data Integrity and Purpose Limitation Principle," which revisits the Safe Harbor's "Data Integrity Prin-

286. Case T-670/16, Digital Rights Ireland v. Data Prot. Comm'r 2016 (General Court filed Sept. 16, 2016).

287. GEERTZ, *supra* note 25, at 232.

288. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 21 (Oct. 6, 2015).

289. The remarks of U.S. Secretary of Commerce Penny Pritzker at the joint conference announcing agreement on the Privacy Shield emphasized these points. *Remarks*, *supra* note 285.

290. U.S. DEP'T OF COM., EU–U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 4 (2016), https://www.privacyshield.gov/EU-US-Framework [https://perma.cc/V2NJ-T6BZ].

ciple."[291] The Privacy Shield adds language, front and center, regarding a requirement of "Purpose Limitation," which telegraphs its increased requirements around compatibility. The Principle also adds specific language, not found in the Safe Harbor, that emphasizes the existence of an "express prohibition on incompatible processing."[292] U.S. companies must now pay greater attention to the collection of personal information from EU citizens and the creation of limits to make only compatible uses of it. Moreover, the increased enforcement mechanisms of the Privacy Shield suggest greater pressure in the future from the EU on companies regarding incompatible uses of information.

"Data integrity and purpose limitation" are also bolstered within the Privacy Shield by a new requirement that restricts "onward transfers" of information.[293] Such transfers to a third party must be for a limited and specified purpose and expressed in business-to-business agreements that provide the same level of protection as the Privacy Shield Principles. In this fashion, the European idea of a state protecting its citizens against bad decisions has been transplanted into international law and U.S. legal mechanisms. Here is a collective mechanism that places limits on individual privacy decision making.

From the perspective of U.S. negotiators, there is mixed news in this result. On the plus side, the language regarding a ban on incompatibility amounts to less than the full-blown EU concept. In EU law, a compatible use must be "specified, explicit, and legitimate."[294] Yet, the language of the Privacy Shield nonetheless moves U.S. companies, if taken seriously and enforced strongly, in a decisive direction towards the idea of "purpose specification."

The second key standard is "choice." The Privacy Shield establishes both opt-out and opt-in rights for the EU data subject whose personal information is being transferred to the United States. It handles opt-in largely in the same fashion as the Safe Harbor. Before the processing of "sensitive data" of an EU citizen, organizations in the United States must obtain "the data subject's affirmative express consent."[295] In other words, the Privacy Shield requires opt-in before processing such information. The concept of sensitive data is a long-established idea in EU data protection law, and a category that the GDPR expands further.[296] U.S. companies must make correct use of stringent EU consent mechanisms. In some instances, such as data processing involving sensitive information, the high requirements for consent will make problematic

---

291. *Id.* at 6.

292. *See id.* ("An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.").

293. *Id.* at 5.

294. GDPR, *supra* note 8, at art. 5(1)(b).

295. EU–U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 290, at 5.

296. The GDPR refers to categories that include "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." GDPR, *supra* note 8, at art. 9(1).

certain kinds of data transfers.[297]

As for opt-out, the Privacy Shield makes an important change to the Safe Harbor's regime. It creates a new category within compatibility that is otherwise unknown to EU data protection law. It envisions a "materially changed, but still compatible" processing operation, which is made subject to an opt-out.[298] This language represents an EU concession to the United States; it accepts the possibility that a "material" change in purpose may nonetheless still be close enough to the original purpose of collection not to require another round of individual consent. As for an *incompatible* use of information, the Privacy Shield explicitly forbids it without new consent. Under EU law, such consent must be specific, collected separately from the initial agreement to processing, and subject to a strict tying restriction.

The Privacy Shield brings the "choice" principle into closer alignment with EU protections for the data subject than the Safe Harbor had done.[299] At the same time, the U.S. negotiators could craft a new category for opt-out, namely that of a material, yet compatible, change in use. Here is a source for future EU–U.S. discussions and possible conflict. The two data privacy regimes are far apart on questions regarding compatibility and purpose specification. In resolving disputes around this issue, mechanisms for enforcement and oversight are critical. They are critical because through these new processes the EU and United States will create new shared concepts regarding compatibility and purpose specification. We now turn to enforcement and oversight.

3. Enforcement

The third set of core principles regards enforcement, and, here, the Privacy Shield marks a considerable change from the Safe Harbor. Enforcement represents the area in the Privacy Shield with the greatest American concessions and the strongest moves in the EU direction. In the words of the European Commission, the Privacy Shield contains strong supervision mechanisms "to ensure that companies follow the rules that they submitted themselves to."[300] The new section concerning redress is termed, "Recourse, Enforcement and Liability Principle."[301] Redress under the Privacy Shield consists of both general enforcement mechanisms and a subset relating only to U.S. intelligence agencies. The general enforcement mechanisms are extensive: the data subject may place a

297. The health care sector in the United States, for example, will face considerable challenges to use of the Privacy Shield and may choose to process personal data of EU citizens solely within the EU. This result follows in part from the strict standards for protecting sensitive data. *See* EU–U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 290, at 9.

298. *Id.*

299. From the U.S. perspective, the Safe Harbor contained weaker and, hence, more desirable language regarding consent.

300. Communication from the Commission to the European Parliament and the Council—Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM (2016) 117 final (Feb. 29, 2016) [hereinafter Transatlantic Data Flows].

301. EU–U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 290, at 7.

complaint with a Privacy Shield company in the United States, complain to their national data protection authority, use alternative dispute resolution if the U.S. company signs up for it, and make use of the "Privacy Shield Panel," an arbitration mechanism that permits binding decisions against U.S. companies.[302]

After the Snowden revelations and the *Schrems* decision, the issue of U.S. government access to the data of EU citizens became a critical issue in Privacy Shield negotiations. The Privacy Shield creates important safeguards regarding U.S. government access to personal data of EU citizens. Among the important changes relating to enforcement is the creation of a U.S. Ombudsperson, who is independent from U.S. intelligence services.[303] The Ombudsperson will respond to individual complaints from individuals who believe that their personal data has been misused by U.S. national security agencies. The Privacy Shield agreement also references important congressional and Executive Branch changes regarding regulation of foreign intelligence surveillance by U.S. agencies.[304] The aim is to document factual changes compared to the record before the *Schrems* court in 2015. The step is a prudent one, taken in anticipation of future litigation in the EU.

4. Oversight

The fourth set of core principles regards oversight.[305] There is now supervision of enforcement procedures by the FTC and the Department of Commerce as well as a specified process to remove companies with insufficient procedures from the Privacy Shield list and to subject them to sanctions.[306] There is also an annual joint review of the Privacy Shield by EU and U.S. officials.[307] Although the Safe Harbor included a limited number of these concepts, the Privacy Shield adds to the oversight list and heightens the overall requirements. To be sure, however, these requirements take the form of political commitments in an agreement with the EU rather than firm statutory obligations through U.S. law. Nonetheless, in the aftermath of *Schrems*, the Privacy Shield necessarily provides strong oversight of the NSA and U.S. intelligence community and provides new ways for EU citizens to obtain redress from the U.S. government as well as private organizations. By comparison, the Safe Harbor did not address national security surveillance.

In sum, the Privacy Shield displays concessions by both sides regarding their own legal models for data privacy. Above all, the document moves the system for data transfers more in the direction of EU data protection law than the Safe

302. Transatlantic Data Flows, *supra* note 300. For the redress mechanisms regarding U.S. intelligence, see *id.*

303. *Id.*

304. *Id.*

305. The oversight principles are primarily anchored in the "Recourse, Enforcement, and Liability" principle. EU–U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 290, at 7.

306. *Id.* at 25–26.

307. *Id.* at 31.

Harbor did. At the same time, from the U.S. perspective, the bottom line for the free flow of data was acceptable. At the press conference in Brussels announcing the Privacy Shield, U.S. Commerce Secretary Penny Pritzker declared that a "free flow of data" was assured "[f]or businesses."[308] Secretary Pritzker added, "For consumers, the free flow of data means that you can take advantage of the latest, most innovative digital products and services, no matter where they originate."[309]

C. CONVERGENCE, DIVERGENCE, AND NEW INSTITUTIONS

A longstanding interest of comparative law scholars is the question of whether the world's legal systems are becoming more or less alike. This assessment is sometimes carried out at a system-wide level, where the analysis is of "families" among the world's legal orders and sometimes, more narrowly, with a focus on discrete substantive areas of law. Working in this latter tradition and writing about data privacy in 1992, Colin Bennett argued that convergence in Europe and the United States had occurred "within a common technological context."[310] More specifically, Bennett proposed that different countries had "converged around statutory principles of data protection, but diverged in policy instruments selected to implement and enforce them."[311]

This Article concludes by updating Bennet's assessment; it identifies current forces for both convergence and divergence. The most important differences from the time of Bennett's analysis, however, are the new institutional structures and processes that the EU and United States have created for harmonizing their approaches to data privacy. In our view, the future path for data privacy will be one of collaboration and concessions. The necessary work will take place within the kinds of "harmonization networks" that Anne-Marie Slaughter has identified as playing a key role in twenty-first century international relations.[312] These are a variety of ad hoc groups that adjust the regulatory standards of multiple countries to achieve an acceptable outcome for all. These networks can also create different mechanisms for compliance in different regulatory systems. The Privacy Shield is only one of the policy improvisations created in the EU and United States to make possible continuing transatlantic data transfers.

1. Convergence

The key forces for convergence in data privacy are the shared technological environment, increased political agreement around the benefits of personal data flow, and common security and law enforcement concerns. To begin with

308. *Remarks*, *supra* note 285.

309. *Id.*

310. COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 150 (1992).

311. *Id.* at 6.

312. ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER 20 (2004).

technology, an important factor for bringing the two systems together is the shared digital environment. The "common technological context" that Bennett found in 1992 is even stronger today. As Bennett concluded at that time, "[t]echnology . . . continues to shape the agenda and to have a common impact."[313]

As in the 1990s, the platforms for computing are largely American in origin. The EU and United States alike use services and products that might be stamped "Made in America" or, more precisely, labeled as "Code from the West Coast." In the late 1980s, Thomas Hughes argued that those who lived in the industrial world inhabited a common "made environment" shaped by the technological systems of that day.[314] Today's "made environment" is created by data-driven digital technology, the presence of which is omnipresent in both America and the EU. Citizens of the EU have also warmly welcomed and enthusiastically adopted each successive wave from the West Coast.[315]

Having helped to fabricate a shared global digital environment, U.S. technology companies now act as force for convergence by seeking accommodation with the EU around questions of government access to data. Post-Snowden, these companies have pivoted from a role as silent helpers of U.S. intelligence agencies to defenders of privacy—at least with respect to demands for their customer data from public authorities.[316] As Henry Farrell and Abraham Newman point out, the involvement of these companies with U.S. national intelligence agencies "badly damaged their corporate reputations and exposed them to foreign sanctions."[317] European customers have not hesitated to make these corporations realize the full extent of their dependency "on free flow of information across borders."[318] One estimate of "lost profits [is] in the billions of dollars" for U.S. tech companies post-Snowden in the EU.[319]

As these companies lost sales in Europe and the glare of publicity about U.S. surveillance continued, these organizations began to distance themselves from the American national security apparatus. The *Microsoft Ireland* litigation marks

313. BENNETT, *supra* note 310, at 247.

314. HUGHES, *supra* note 262, at 184.

315. Facebook is a good example of the EU interest in U.S. social media with a 102% rate of growth in use in the EU from 2010 to 2016. *Facebook Users in the World*, INTERNET WORLD STATS (June 2016), http://www.internetworldstats.com/facebook.htm [https://perma.cc/6P5A-7NPK].

316. *See, e.g.*, Jacob Gershman, *For Google's Data Wars, It All Comes Down to Location*, WALL ST. J. (Apr. 3, 2017), https://www.wsj.com/articles/for-googles-data-wars-it-all-comes-down-to-location-1491217202 [https://perma.cc/7L3R-MSDK] ("Google and the Justice Department are clashing in courtrooms across the country over the government's power to compel the company to turn over emails and other personal data sought in criminal probes.").

317. Farrell & Newman, *supra* note 4.

318. *Id.*

319. Ned Schultheis, *Warrants in the Clouds: How Extraterritorial Application of the Sotred Communications Act Threatens the United States' Cloud Storage Industry*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 664 (2015). Schultheis observes that U.S. technology companies are "still reeling from international damage caused by Edward Snowden's mass leak." *Id.* at 663.

a turning point in this regard.[320] Pursuant to the Stored Communications Act, U.S. law enforcement officials requested information stored in a Microsoft data center in Ireland. Microsoft refused disclosure and took the path of high profile and, thus far, successful litigation.[321] Other leading U.S. technology companies are similarly resisting law enforcement demands for information.[322]

Just as U.S. companies are taking a more EU-friendly approach in some areas, some European policymakers are interested in modifying their law to accommodate certain aspects of U.S. information privacy law. The continent and EU benefit greatly from the flow of data in global networks. As an illustration of a new awareness of these benefits, German Chancellor Angela Merkel called in November 2016 for adaption of European data protection to the age of Big Data.[323] In her view, European industry should be able to do more with personal information than data protection currently permits.[324] The powerful German auto industry is said to be in the front ranks of lobbying for such changes; its goal is to be able to play a central role in the development of "connected cars." This industry views the future of next-generation automobiles as dependent on access to the personal data of drivers; the concern is that European data protection law will disadvantage it vis-à-vis its competitors in the United States and elsewhere.[325]

The EU negotiators for the Privacy Shield also understood the importance of digital economic transactions. The Commission wishes to demonstrate that it can manage economic relations and protect fundamental rights. As it noted after the successful conclusion of the Privacy Shield negotiations, this Treaty "demonstrates the EU's capacity to solve problems in a pragmatic and focused manner without sacrificing its strong fundamental rights values and traditions."[326] As further indication of this interest in data sharing, the Commission is developing an initiative to promote a Digital Single Market and one where it seeks to make

320. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 474–75 (S.D.N.Y. 2014).

321. For an analysis of this litigation, see Paul M. Schwartz, Microsoft Ireland *and a Level Playing Field for U.S. Cloud Companies*, 15 PVLR 1549 (Aug. 1, 2016).

322. As Orin Kerr sums up the landscape for Internet providers, "Privacy is big business right now, especially in Europe." Orin Kerr, *The surprising implications of the Microsoft/Ireland Case*, WASH. POST: THE VOLOKH CONSPIRACY (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case [https://perma.cc/H6LJ-PM5R].

323. *Merkel Calls for Balanced Approach to Data Protection*, REGISTER (Nov. 22, 2016), http://www.theregister.co.uk/2016/11/22/merkel_data_protection_big_data/ [https://perma.cc/3AQS-4UTC].

324. *Id.*

325. On the lobbying for these changes to EU privacy law by German auto manufacturers, see Derek Scally, *Minister 'Heartened' by Merkel Shift on Data Privacy Laws*, IRISH TIMES (Nov. 25, 2016), https://www.irishtimes.com/business/technology/minister-heartened-by-merkel-shift-on-data-privacy-laws-1.2882211 [https://perma.cc/KN2D-8N5Y]. On activities of German automakers involving connected cars, see William Boston, *Intel Buying 15% Stake in Here, German Auto Makers' Digital-Map Venture*, WALL ST. J. (Jan. 3, 2017), www.wsj.com/articles/intel-seeks-approval-to-invest-in-german-auto-makers-digital-mapping-venture-1483458002 [https://perma.cc/STR6-NKUR].

326. Transatlantic Data Flows, *supra* note 300.

"digital a driver for growth."[327]

A final force for convergence is international security. This prediction is perhaps surprising considering the folk hero status of Edward Snowden on much of the continent.[328] In our view, however, the EU and United States are currently passing through a brief unsettled period around surveillance issues after disturbance of the previous status quo. Longer term, the similar regulation of intelligence agencies in the EU and United States and shared security concerns are likely to support development of new agreements in this area. This point deserves elaboration.

To begin with, EU member states boast their own intelligence agencies, whose practices are at least roughly similar to those of the United States.[329] Indeed, both before and after Snowden, intelligence services in EU member states benefited from U.S. surveillance capabilities, carried out their own intelligence activities, and, in some cases, maintained data sharing arrangements with the NSA.[330] There is also ongoing legislative activity in EU member states to bolster the data-gathering powers of intelligence and law enforcement agencies. Among EU member states, France has taken a particularly active role in expanding surveillance powers for its intelligence agencies and law enforcement.[331] As for the judiciary, the European Court of Justice concedes that issues of national security and criminal justice fall outside the scope of EU law.[332] In a similar fashion, the European Court of Human Rights has not taken a strong role in limiting the power of national security agencies. As two analysts note, the caselaw of the Strasbourg court establishes only "minimum common rules" for security and law enforcement.[333]

Finally, the EU and United States have shared concerns regarding international terrorism and organized criminality.[334] EU data protection need not stand in the way of transatlantic cooperation in this area. Indeed, the EU's own data protection law does not extend to activities concerning its members' national

---

327. *Id.*

328. As an example, a paperback published in Germany termed itself a "homage to the most important whistleblower of the world," MARC HALUPCZOK, 111 GRUNDE EDWARD SNOWDEN ZU UNTERSTUTZEN (2014) [111 Grounds to Support Edward Snowden].

329. A good overview of these capabilities is found in a special volume of International Data Privacy on systematic government access to private-sector data. *See* Fred H. Cate et. al, *Systematic Government Access to Private-Sector Data*, *in* 2 IDPL 195 (2012). For a specific country report, see Paul M. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, *in* 2 IDPL 289 (2012). Updated versions of these reports will be published in BULK DATA (Fred H. Cate & James X. Dempsey, eds., forthcoming 2017).

330. *See* David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide: The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INT. J. CONST. L. 220, 222 (2016) ("At the end of the day, the EU and the US may well be converging more than diverging with respect to national security surveillance.").

331. Winston Maxwell, *Systematic Government Access to Private-Sector Data in France*, 4 INT'L DATA PRIVACY L. 4 (2014)

332. Cole & Fabbrini, *supra* note 330, at 222.

333. *Id.* at 225.

334. *Id.* at 223.

security. These activities manage to be both part of the "common foreign and security policy of the Union," but also to fall "outside the scope of Union law" as far as data protection is concerned.[335] As Recital 16 of the GDPR explicitly states, "This Regulation does not apply to . . . activities concerning national security."[336]

As an example of shared transatlantic concerns, EU Justice Commissioner Věra Jourová has taken a leadership role not only regarding the annual review of the Privacy Shield but also, within the EU, in seeking to guarantee police access to encrypted information on such messaging apps as WhatsApp and Signal. Following a terrorist attack in London outside the House of Commons in March 2017, Interior Ministers throughout the EU called for laws to guarantee police access to encrypted online communications.[337] Backing these demands, Jourová stated that there was a need for "a swift, reliable response" when law enforcement demanded encrypted information.[338] Here is a transatlantic echo of the kinds of warnings that FBI Director James Comey had made in the United States of the growing dangers of "going dark."[339] Comey used this term to depict a world in which U.S. law enforcement and intelligence agencies have lawful authority but due to encryption were not able "to access the evidence we need to prosecute crime and prevent terrorism."[340]

As a further example of shared law enforcement concerns, both sides of the Atlantic are concerned about continuing access to cloud data. In the United States, the government has enjoyed a mixed record in use of the Stored Communications Act to gain such access to extraterritorial cloud data.[341] Following terroristic acts in Manchester and London in June 2017, Jourová called for new legislation to permit speedier access by law enforcement to cloud data in Europe.[342] She expressed her certainty that "there will be more understanding"

---

335. GDPR, *supra* note 8, at Recital 16.

336. *Id.*

337. Patricia Howell O'Neil, EU Justice Commissioner, *New 'Options' on Encrypted Communications Access Are Coming*, CYBERSCOOP (Mar. 30, 2017), https://www.cyberscoop.com/eu-encryption-backdoors-vera-jourova [https://perma.cc/EB35-GL2X].

338. *Id.*

339. James B. Comey, Speech, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/N5ST-KM5U].

340. *Id.*

341. *See, e.g.*, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 229 (2d Cir. 2016), *reh'g en banc denied*, 855 F.3d 53 (2d Cir. 2017); *In re* Information Associated with [Redacted]@gmail.com, 2017 WL 3445634 (D.D.C. July 31, 2017); *In re* Two Email Accounts Stored at Google, Inc., 2017 WL 2838156 (E.D. Wisc. June 30, 2017); *In re* Search of Content that is Stored at Premises Controlled by Google, 2017 WL 1398279 (N.D. Cal. April 19, 2017); *In re* Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *In re* Search Warrant No. 16-960-M-01, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017).

342. Samuel Gibbs, *EU Could Give Police Direct Access to Cloud Data in Wake of Terror Attacks*, GUARDIAN (June 8, 2017), https://www.theguardian.com/technology/2017/jun/08/european-union-police-direct-access-cloud-data-terror-attacks-threats.

among EU justice ministers of the need for such a measure "in the shadow of the recent terrorist attacks and increasing threats in Europe."[343]

There are also signs of increased transatlantic cooperation around these issues, including the signing of a new EU–U.S. data protection "Umbrella Agreement" in June 2016 to permit information sharing to "to combat crime, including terrorism."[344] The Umbrella Agreement establishes data privacy protections for all personal data that is shared pursuant to it.[345] As this new bilateral data protection agreement demonstrates, much room is open for cooperation between the United States and the EU as well as with member states. In sum, there are indications that a new post-Snowden status quo around issues relating to national security surveillance can be reached.

2. Divergence

Although pressure exists in the EU and United States for convergence around some data privacy issues, there are also forces for divergence. In 1992, Bennett had already identified the varying legal instruments in the EU and United States.[346] Today, there are still omnibus laws in the EU and a patchwork of sectoral ones in the United States. Of greater significance, in our view, are the different conceptions of legal identity in the two systems. In the EU, rights talk seeks to create a new political identity—that of the European citizen. Rights talk also has important institutional dimensions. The constitutionalization of data protection has occurred through national constitutional courts in member states and transnational courts, namely, the European Court of Human Rights and the European Court of Justice. The EU constitutional courts, supranational and national, have been actively engaged in protecting human dignity and self-determination against the inroads of personal data processing. As Fabbrini argues, the overlap of judicial institutions and instruments creates "an incentive for expansion" of fundamental rights.[347] No similar constitutional interests exist in the United States, and no incentive is present to encourage expansion of the limited privacy rights that do exist.

Regarding remedies, this area is likely to be one of increasing divergence between the two systems. In the EU, bedrock principles regarding harm and standing differ greatly from the United States. The collection, use, or transfer of personal data in the EU implicates an individual's dignity and self-determination and requires a basis in law. Without such a legal basis, the processing of personal data harms a legal interest of the individual. This concept is safeguarded through EU constitutional law, the Directive, and now the GDPR. The

343. *Id.*

344. *Signing of the "Umbrella" Agreement: A Major Step Forward in EU-U.S. Relations*, EUROPEAN COMMISSION (June 2, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm [https://perma.cc/RB6G-RP4Y].

345. *Id.*

346. BENNETT, *supra* note 310, at 152–54.

347. FABBRINI, *supra* note 42, at 13–14.

system also guarantees assistance from an independent national data privacy commissioner. In contrast, the United States has a highly uncertain sense of privacy remedies, and the pendulum appears to be swinging towards an even more restrictive view of redress. Indeed, one observer predicts that the FTC will soon be limiting its enforcement actions to pecuniary harms based solely on "economic injuries."[348]

Another important aspect of remedies is that of standing. In the EU, data protection law permits legal claims for both "material or non-material damage" if its requirements are not followed.[349] In the United States, in *Spokeo*, the Supreme Court opened the door for a constitutionalization of "privacy harms."[350] By preventing consumers from suing under existing sectoral laws that permit recovery based on statutory violations, the Supreme Court may be starting down the road to a new "*Lochner*-ization" of legislative power.[351] For the *Lochner* Court, a state law limiting the working hours of bakers was an unconstitutional infringement of their freedom of contract. The Supreme Court ultimately rejected this idea in *West Coast Hotel v. Parrish*: the state is free to regulate economic activities, and the Due Process Clause is not to be used to strike down laws in the name of freedom of contract.[352] As in *Lochner v. New York*, however, the Supreme Court again appears ready to identify requirements in the Constitution, namely in Article III, that will limit the ability of legislatures to protect individuals.[353]

As for contract and consent, there is ample room for misunderstandings and disagreements between the two systems about these doctrines. In the future, if the United States seeks greater use of consensual mechanisms to justify international data transfers, the EU is likely to resist. Where U.S. policymakers see sovereign consumers, EU policymakers worry about a data subject confronted by power imbalances and overwhelmed by impenetrable legalese in privacy notices and terms of service. The EU acts as well to prevent a negative impact on democratic values by limiting certain choices. Deeply-rooted issues of legal identity tug in different directions in the EU and United States.

Finally, there is the "Trump Effect" as a possible force for divergence between the EU and United States. President Donald Trump has the potential to destabilize current relations between the EU and United States. His inconsistent remarks regarding the worth of NATO and his apparent refusal to shake hands at a meeting with Angela Merkel, Chancellor of the Federal Republic of Germany, are examples of behavior unlikely to enhance the trust felt by key

348. HOOFNAGLE, *supra* note 123, at 345.
349. GDPR, *supra* note 8, at art. 82(1).
350. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016).
351. Lochner v. New York, 198 U.S. 45 (1905).
352. 300 U.S. 379, 392–93 (1937).
353. Some lower courts are already relying on *Spokeo* to deny privacy claims. For a sampling of such decisions, see Nicklaw v. Citimortgage, Inc., 839 F.3d 998 (11th Cir. 2016); Braitberg v. Charter Commc'ns, 836 F.3d 925 (8th Cir. 2016); Hancock v. Urban Outfitters, 830 F.3d 511 (D.C. Cir. 2016).

European allies.[354] Less than six months after President Trump took office, a poll in Germany, a vital ally of the United States, found that 74% of the public agreed with the statement that the United States could not be trusted.[355] This result tied the United States with Russia regarding the relative level of distrust that Germany felt towards the other nation.[356] More specifically concerning data privacy, there are three areas of concern.

First, the Privacy Shield is not simply one document, but a discrete suite of agreements. An important part of this cluster is Presidential Policy Directive (PPD) 28 concerning signals intelligence, which the Obama Administration approved on January 17, 2014.[357] Under it, President Obama extended certain privacy protections to non-U.S. citizens when subject to foreign intelligence surveillance. PPD 28 declares that "all persons should be treated with dignity and respect regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information."[358] This order develops a list of policies and procedures, including data minimization, which "are to be applied equally to the personal information of all persons, regardless of nationality."[359] This Directive can be swept away, however, through a signature of President Trump, who might view it as inconsistent with his "America First" approach.[360] In a similar fashion, many of the oversight mechanisms on the U.S. side of the Privacy Shield are dependent on U.S. political commitments rather than statutory law. Hence, they are vulnerable to a change in the Executive Branch in the way that enacted federal law is not.

Second, with the Privacy Shield arrangement, the United States sought to correct the record before the *Schrems* court about American surveillance practices and to provide new institutional procedures for intelligence oversight, including bilateral methods for shared oversight with the EU. President Trump is now indirectly undermining EU trust in this arrangement. He is doing so through persistent evidence-free claims that President Barack Obama and others "wiretapped" him during the 2016 presidential campaign.[361] Such claims sug-

354. James Rothwell & Barney Henderson, *Donald Trump Refuses to Shake Angela Merkel's Hand as Key Meeting Gets Off to Frosty Start*, TELEGRAPH (Apr. 8, 2017), http://www.telegraph.co.uk/news/2017/03/17/donald-trump-meet-angela-merkel-white-house-make-break-meeting [https://perma.cc/54VE-S8R9].

355. Ellen Ehni, *Deutschlandtrend: Schulz unten, Merkel obenauf*, TAGESSCHAU.DE (June 8, 2107) https://www.tagesschau.de/inland/deutschlandtrend-809.html [https://perma.cc/446D-PGAY].

356. *Id.*

357. Signals Intelligence Activities, Presidential Policy Directive 28 (January 17, 2014).

358. *Id.* at 1.

359. *Id*. at 5.

360. For a bipartisan plea for Trump to preserve PPD 28, see Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE (Jan. 17, 2017), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/W4RN-CSHA].

361. Michael Shear & Michael Schmidt, *Trump, Offering No Evidence, Says Obama Tapped His Phones*, N.Y. TIMES (Mar. 4, 2017), https://www.nytimes.com/2017/03/04/us/politics/trump-obama-tap-phones.html [https://perma.cc/3KJD-AG2M].

gest that surveillance activities in the United States are subject to presidential fiat. President Trump is also casting doubt on the worth of any promises to the EU from the U.S. intelligence community regarding whether it follows its promises regarding data transfers involving EU citizens.[362] He is undercutting the value of guarantees from the U.S. intelligence community by disagreeing with official assertions to the contrary regarding any wiretapping of him during the campaign.[363]

Third, the Privacy Shield depends on a complex structure in which the United States and EU monitor U.S. intelligence activities. As part of this oversight, the Shield creates a new position, the Privacy Shield Ombudsman, who is to be independent of the U.S. intelligence community and is "to provide redress in the area of national security for EU citizens."[364] In addition, the Shield depends on the ongoing work of the Privacy and Civil Liberties Oversight Board (PCLOB), an existing independent, bipartisan agency in the Executive Branch. For the EU, the PCLOB is an important part of the multiple oversight layers in place for the U.S. intelligence community.[365] There is a risk, however, that the Trump Administration will undermine the Privacy Shield by failing to maintain these two parts of its institutional structure. Thus far, it has failed to fill the position of the Ombudsman permanently and has delegated the requisite duties to an Acting Assistant Secretary of State. It has also nominated only one new member to the PCLOB, which, as of September 2017, was down to a single member instead of five and could be considered "essentially defunct."[366] This threat of the degradation of institutional capacities matters because of the central future role of varied transatlantic organizations in generating shared understandings of data privacy.

---

362. The Commission's Implementing Decision to the Privacy Shield found that "U.S. law ensures that surveillance measures to obtain foreign intelligence information . . . and [are] tailored as much as possible." Commission Implementing Decision Privacy Shield 24 (July 12, 2016), C(2016) 4176 final.

363. Trump's claims that Obama wiretapped him have been refuted by the FBI Director, the heads of congressional Intelligence Committees, the past Director of National Intelligence, and the current Director of the National Security Agency. Peter Baker & Charlie Savage, *Trump Digs In on Wiretap, No Matter Who Says Differently*, N.Y. TIMES (Mar. 16, 2017), https://www.nytimes.com/2017/03/16/us/politics/richard-burr-mark-warner-trump-wiretap.html?_r=0 [https://perma.cc/TDV3-5F2A]. Finally, in September 2017, in response to a Freedom of Information Act request, the DOJ stated that it had no evidence to support President Trump's assertion that Obama wiretapped the phones in Trump Tower before the election. Deirdre Walsh, *Justice Department: No Evidence Trump Tower Was Wiretapped*, CNN (Sept. 3, 2017, 5:50 PM), http://www.cnn.com/2017/09/02/politics/justice-department-trump-tower-wiretap/index.html [https://perma.cc/4PSX-HTXE].

364. EU–U.S. Privacy Shield, Frequently Asked Questions, European Commission (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm [https://perma.cc/XEH8-2YLQ]; Commission Implementing Decision Privacy Shield, *supra* note 362, at 17.

365. Commission Implementing Decision Privacy Shield, *supra* note 362, at 25.

366. Natasha Lomas, *EU–U.S. Privacy Shield Remains Precariously Placed*, TECHCRUNCH (Apr. 6, 2017), https://techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed [https://perma.cc/W7AQ-D6CY]. Regarding the nomination of Adam Klein to be Chairman of the PCLOB, see Susan Hennessey, *White House to Nominate Adam Klein to the PCLOB*, LAWFARE (Aug. 28, 2017, 4:49 PM), https://lawfareblog.com/white-house-nominate-adam-klein-pclob [https://perma.cc/3QN3-645X].

3. New Institutions and New Structures

In 1924, Cardozo described the function of law as a marker of social consensus. He argued that law is an "agreement about the things that are fundamental."[367] Comparative law permits an evaluation of whether different legal systems are in accord or discord about "things that are fundamental." This Article has argued that the EU and United States start with profoundly different perspectives on the individual as bearer of privacy interests. But a novel set of doctrines and institutions in the EU and United States are now tasked with developing this area of law. These institutions represent a fresh way for the EU and United States to reach agreement about "things that are fundamental." We now return to the question of interoperability and the White House's goal of "mutual recognition" around "common values surrounding privacy and personal data protection."[368]

In our view, the future for data privacy will not be driven by a "Brussels Effect" based on de facto unilateralism.[369] Here, we disagree with Anu Bradford, who sees the EU as successfully having exported its standards in many legal and regulatory domains through de facto unilateralism.[370] Rather than a "Brussels Effect," international data privacy law now features the kinds of "harmonizing networks" that Anne-Marie Slaughter identifies as a key factor for international relations in the twenty-first century. In the place of foreign ministries and state departments, the traditional locus of international relations, new kinds of "disaggregated state institutions" work today in an ad hoc manner through a variety of regulatory, judicial, and legislative channels.[371] Slaughter observes, "The more that international commitments require the harmonization or other adjustment of domestic law, the coordination of domestic policy, or cooperation in domestic enforcement efforts, the more they will require government networks to make them work."[372] As recent work by Slaughter indicates, moreover, the resulting networks can take a complex form. Such a hub can anchor "an overlapping set of groups, clubs, and associations of all actors dedicated to addressing a particular set of issues."[373]

The GDPR and Privacy Shield create the most important of the new institutions and processes for potentially facilitating interoperable privacy regimes. Indeed, even after Brexit, the U.K. appears fully committed to following the GDPR, with the May government confirming it will implement it.[374] The future

367. BENJAMIN N. CARDOZO, THE GROWTH OF THE LAW 144 (1924).

368. CONSUMER DATA PRIVACY, *supra* note 16, at 31.

369. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 8 (2012).

370. *Id.*

371. SLAUGHTER, *supra* note 312, at 5.

372. *Id.* at 162.

373. ANNE-MARIE SLAUGHTER, THE CHESSBOARD AND THE WEB 223 (2017).

374. BBC News, *Queen's Speech: new data protection law*, BBC (June 21, 2017) http://www.bbc.com/news/technology-40353424 [https://perma.cc/E7XX-YYD7]; Elizabeth Denham, *How the ICO will be supporting the implementation of the GDPR*, INFO. COMMISSIONER'S OFF. BLOG (Oct. 31, 2016),

of transatlantic data trade will turn on concessions and compromises within this framework, which is more diffuse and offers more points of contact than before. This Article now takes inventory of this structure by drawing on a model identified by Ryan Goodman and Derek Jinks.[375] In the Goodman–Jinks paradigm, there are three distinct mechanisms through which states seek to influence the practice of other states and institutions. These approaches to influence are coercion, persuasion, and acculturation.[376] This classification proves helpful in thinking about how the EU and United States might continue to "agree to disagree" about certain fundamental aspects of data privacy, but also develop a successful regime for international data transfers.

The GDPR demonstrates all three aspects of the Goodman–Jinks model. First, it does not shy away from creating powers of coercion for EU privacy policymakers. The most important such tool for coercion is one that was already present in the Directive: the ability to restrict personal data transfers to non-EU countries that lack "adequate" privacy protections.[377] As Goodman–Jinks explain their concept of "coercion," it escalates the "benefits of conformity or the costs of nonconformity through material rewards and punishment."[378]

Since 1995, European data protection law has provided such a coercive power for itself. On the benefit side, it has created a "white list" of non-EU nations that it has found to have "adequate" data protection. On the cost side, it requires more of public and private sector entities in countries not on this list, namely, an ability to demonstrate adequacy in the processing of personal data. At the same time, the EU has been careful to seek other ways to influence the behavior of non-EU nations and organizations. It has turned to powers of persuasion and acculturation.

Second, the GDPR provides good examples of the EU structuring interactions with non-EU countries around persuasion. The GDPR assigns power to the Commission to "enter into consultations" with third countries that may no longer ensure an adequate level of protection.[379] Such consultations occur in a formal institutional environment in which the target audience is, as Goodman–Jinks might put it, "cued" to consider the merits of the EU's message.[380] For example, the GDPR's Article 50 calls for international mutual assistance, the engagement of international stakeholders with each other, and the development of "international cooperation mechanisms to facilitate the effective enforcement

---

https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr [https://perma.cc/86V9-Q69B]. For a discussion in the academic literature in the U.K., see William Malcolm, *Overseas or Cross-Border Transfers of Personal Data: Schrems, Brexit, and the General Data Protection Regulation*, *in* GUIDE TO THE GENERAL DATA PROTECTION REGULATION 143, 154–56 (Rosemary Jay, ed., 2017).

375. Goodman & Jinks, *supra* note 24, at 621.

376. *Id.* at 623–25.

377. GDPR, *supra* note 8, at art. 5.

378. Goodman & Jinks, *supra* note 24, at 633.

379. GDPR, *supra* note 8, at art. 45(6).

380. Goodman & Jinks, *supra* note 24, at 637.

of legislation for the protection of personal data."[381] These parts of the GDPR demonstrate the EU's commitment to shaping data privacy law through international dialogue based on deliberation and argument. Moreover, the EU imbeds these discussions in the kind of networks that Slaughter identifies as critical to twenty-first century international relations.

Some of these networks are created by the Privacy Shield, which is the kind of multistakeholder entity that the White House envisioned in 2012 as a key part of global privacy policymaking. Perhaps the most innovative aspect of the Privacy Shield is that it "deputizes" U.S. institutions, officials, and private parties to enforce the interests of EU citizens and to do so accompanied by EU oversight. To safeguard the interests of EU citizens, Privacy Shield companies are to establish Alternative Dispute Resolution processes; the FTC and State Department are to resolve complaints by these parties; and an independent Ombudsperson is to interact with U.S. national security agencies.[382] Among other entities, the PCLOB is to help oversee the U.S. intelligence communities. There is also a process for the Commission and Department of Commerce to collaborate on an annual joint review.[383]

There is recourse to the mechanisms of persuasion and acculturation in the Privacy Shield, and we begin with persuasion. Officials and individuals in the EU and United States are now part of a disaggregated network tasked with devising new solutions for harmonizing their underlying views of data privacy. This environment creates varying degrees of formal pressures on behavior and cognition to adopt conforming results. The result is a disaggregated process for joint EU–U.S. "lawmaking." This resulting sharing of power will occur, for example, in future decisions about novel doctrinal concepts, such as that of a "material change" in the grounds for processing that is still "compatible." [384]

Moreover, the process of annual EU–U.S. reviews formalizes the conditions for regular "persuasive encounters," in which norms are elaborated and given more concrete form.[385] EU officials will have ample opportunities to create pressure against the kinds of potential neglect, if not outright intentional impairment, of U.S. privacy institutions that appears to be occurring under the Trump Administration. During an April 2017 visit to the United States, for example, EU Commissioner Jourová warned that the EU considered PCLOB to be one of the "essential" elements for "the sustainability of the Privacy Shield."[386]

Finally, we come to acculturation in the Privacy Shield. This agreement provides ample opportunities for acculturation of parties from the EU and United States as members of a new community. There is the potential for each side to work together to generate new global privacy norms and to diffuse them

381. GDPR, *supra* note 8, at art. 50(1)(a).
382. Transatlantic Data Flows, *supra* note 300.
383. *Id.*
384. EU–U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 290, at 6.
385. Goodman & Jinks, *supra* note 24, at 680.
386. Lomas, *supra* note 366.

back within their own system. Here, our focus can shift to the nearly two thousand U.S. companies that have already entered the Privacy Shield.[387] These companies have voluntarily agreed to practice European-style data protection for information received pursuant to data transfers from an EU member state. This activity helps shape the parameters by U.S. participation in a global community of privacy professionals.[388]

This globalization of privacy compliance work has led to ongoing interactions among those lawyers, policymakers, and others engaged in this area. As Kenneth Bamberger and Deirdre Mulligan have demonstrated through a series of wide-ranging field interviews, chief privacy officers and other privacy professionals are now "embedded in a shared community, tethered to a common logic and shared purposes: privacy and its protection."[389] Without formal recourse to the Goodman–Jinks terminology, Bamberger and Mulligan have independently identified the strong force of acculturation within this community. In it, shared values are now created "through negotiation, disagreement, as well as advice, encouragement, and constructive criticism."[390]

In short, like the Safe Harbor before it, the Privacy Shield creates a normative infrastructure for bringing EU-style privacy practices into the United States. Another EU mechanism for transatlantic data transfers, Binding Corporate Rules, requires a company to provide EU data protection throughout its entire corporate structure for all intraorganizational transfers of personal data across borders.[391] These processes create a force for acculturation and conformity within a global community of privacy professionals.

Ultimately, it is an established institution, the European Court of Justice, that will have the final word on the outcome from these institutions and processes. Pursuant to *Schrems*, in evaluating EU–U.S. law around data transfers, including the Privacy Shield, the European Court of Justice must determine whether the resulting protections are "essentially equivalent" to those required of EU member states.[392] There is a major difference, however, today compared to the legal landscape under the Safe Harbor. Once it was approved, the Safe Harbor was a static document with scant opportunity for input from EU officials. In contrast, the Privacy Shield can evolve in a more dynamic fashion with greater opportunities for policy involvement by EU data protection officials and more chances for alterations to it.

---

387. For the list, see Privacy Shield Framework, https://www.privacyshield.gov/list [https://perma.cc/DJY5-YZMX].

388. BAMBERGER & MULLIGAN, *supra* note 275.

389. *Id.* at 229.

390. *Id.*

391. *Binding Corporate Rules*, European Commission (Apr. 7, 2017, 2:38 PM), http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm [https://perma.cc/B43K-TW5G]. For a discussion, see SOLOVE & SCHWARTZ, *supra* note 30, at 270–71.

392. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650, ¶ 21 (Oct. 6, 2015).

There can be some hope, therefore, that the European Court of Justice in its future assessments will operate in a fashion like Europe's national constitutional courts. In the analysis of Stone Sweet, these courts frequently enable corrective processes that bring other governmental bodies into dialogue with it.[393] They often favor judgments that permit "corrective revision efforts" and only "partial victories."[394] With more EU officials involved in U.S. "lawmaking" around data privacy than in the pre-Snowden landscape, the European Court of Justice may be more forgiving of the Privacy Shield than it was of the Safe Harbor. At any rate, as demonstrated by *Schrems*, the European Court of Justice will continue to be a powerful force for shaping international data privacy law.

CONCLUSION

As a concluding attempt to further a sympathetic understanding of the EU's belief system around privacy, we wish to go beyond legal sources and reference Mercer, a character in THE CIRCLE (2013), a novel by Dave Eggers, an American writer. Mercer is doubtful of the unbridled blessings of technology and a culture that encourages people to surrender their personal data. More specifically, he is concerned about his friend Mae, who is enamored of life at her technology company, which encourages oversharing (to put it mildly). Mercer makes this passionate plea to Mae: "*Individually* you don't know what you're doing *collectively*."[395]

In placing limits on certain possible choices, EU data protection has acted to restrict the collective negative impact of individual trade in personal information.[396] It has sought to resolve the quandary that Mercer identifies, which is the collective negative impact of unbridled individual decisions. The EU has constructed a legal identity for its citizens around rights protection and promoted a democratic culture that rests on informational self-determination. It has strong constitutional protections in place and omnibus laws that restrict the sweep of contract and consent. In contrast, the United States lacks any similar constitutionalization of its information privacy law and proceeds through a sectoral legislative approach. The United States is interested in the free flow of data and access to the bounty from the consumer marketplace. These goals have led to strong efforts to protect the data marketplace for privacy consumers.

Law ultimately survives only as far as it serves social purposes and will be reshaped to accord with those goals. At a high level, the EU and United States recognize the value of both data privacy and the free flow of information.

393. SWEET, *supra* note 40, at 82.

394. *Id.* at 142.

395. EGGERS, *supra* note 261, at 267.

396. Several American legal scholars have long adopted this perspective. Among these scholars are Julie Cohen, Neil Richards, Paul Schwartz, and Daniel Solove. In their respective scholarship, this group has called on U.S. lawmakers to consider "the social impacts of individual privacy decisions." Solove, *supra* note 257, at 1892. Their call has enjoyed about as much impact on U.S. law as Mercer's plea to Mae, which is to say none.

International privacy policymakers now have new structures for deciding how to achieve both goals and for reshaping the law. The question of privacy's international future turns on whether the two systems can bridge the differences about the "things that are fundamental" in each of their legal cultures. Ultimately, the need is for both sides to acknowledge the existence of their differences while working within the new framework for structured engagement. Both the GDPR and Privacy Shield require regular interactions between the EU and United States with numerous opportunities for harmonization, coordination, and cooperation. These legal documents offer a fresh start for the EU and United States in resolving conflicts about data privacy.