Structuring International Data Privacy Law

By Paul M. Schwartz[*] & Karl-Nikolaus Peifer[**]

I. Introduction

Due to the significance of international flows of personal information, the stakes are high today for the European Union and the United States when it comes to data privacy law. According to one estimate, the U.S.-EU economic relationship involves $260 billion in annual digital services trade.[1] Cross-border information flows represent the fastest growing component of U.S. as well as EU trade.[2] In today's information economy, moreover, much of this U.S.-EU trade involves personal data. As one reporter on the tech beat noted, "International data transfers are the lifeblood of the digital economy."[3]

The sharing and use of personal information now drive many daily activities, including finances, health care, shopping, telecommunications, and transportation. Leading U.S. technology 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. Differences in transatlantic regulations potentially imperil these critical international data flows.

The resulting EU-U.S. dispute has been termed the "transatlantic data war."[4] The roots of this "war" are found in the differing legal approaches to information privacy in the two jurisdictions. There has also been a longstanding debate in the EU 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.[5] This policy debate has been accompanied by the EU setting strict limits

---

[*] Jefferson E. Peyser Professor of Law at UC Berkeley School of Law; Director, Berkeley Center for Law & Technology. The authors would like to thank the Thyssen Foundation for their support of this Article.

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

[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.

[2] Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy, SWD (2017) 2 final (Jan. 10, 2017).

[3] 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?_r=0.

[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.

[5] Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995).

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 European Directive on Data Protection (1995) permits data transfers from the EU to a third party nation only when it has "adequate" privacy protections.[6] On May 25, 2018, the General Data Protection Regulation (GDPR) (2016) will take the place of the Directive.[7] Under the GDPR, the adequacy requirement for data transfers continues to be the legal touchstone. The EU has never considered U.S. data privacy law to have an adequate level of protection.[8]

In response to the EU's judgment that the privacy protections of U.S. law were insufficient, the EU and U.S. developed a set of first-generation solutions for transatlantic exchanges. Due to EU displeasure with the surveillance of the National Security Agency (NSA), however, these innovative mechanisms are now either invalid or imperiled.[9] An initial second-generation solution, the EU-US Privacy Shield, was finalized in June 2016.[10] There are already legal challenges to it in progress in the EU.[11]

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. The White House and Federal Trade Commission have promoted this approach. For the White House, there is a need for a "multistakeholder process" with the international partners of the U.S. to "facilitate interoperable privacy regimes."[12] These regimes are to be based on the starting point of "mutual recognition," which entails an "embrace of common values surrounding privacy and personal data protection."[13]

---

[6] Council Directive 95/46, art. 25, 1995 O.J. (L 281) 31, 45–46 (EC) [hereinafter DP Directive].

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

[8] *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) (stating regarding U.S. privacy law that "the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot be relied upon to provide adequate protection" for data transferred from EU).

[9] The decisive move was made in 2015 by the European Court of Justice's *Schrems* decisions, which invalidated the Safe Harbor Agreement between the EU and U.S. Case C-362/14, Schrems v. Data Prot. Comm'r 2015 E.C.R. 650 (Oct. 6, 2015).

[10] 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 [hereinafter Privacy Shield, Implementing Decision], http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

[11] 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.

[12] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 31-32 (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter CONSUMER DATA PRIVACY].

[13] *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 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

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 U.S. It identifies profound differences in the two system's image of the individual as bearer of legal interests. The EU has created a privacy culture around "rights talks" that serves to protect "data subjects."[14] In the U.S. in contrast, the focus is on "marketplace discourse" about personal information and the safeguarding of "privacy consumers."[15] In the EU, moreover, "rights talk" forms a critical part of the post-war 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.[16] In the U.S., in contrast, data privacy law is based on the idea of consumers whose interests merit governmental protection in a marketplace marked by deception and unfairness.

This Article uses its models of "rights talk" and "marketplace discourse" to analyze how the EU and the U.S. protect their respective data subjects and privacy consumers. A particular focus is on the respective doctrines of consent and contract in the two legal systems, which reflect profoundly different perspectives. Even if 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. This Article argues that the future of international data privacy rests not in unilateralism, whether from the EU or U.S., but in these myriad new venues for collaboration. Both the GDPR and Privacy Shield require regular interactions between the EU and U.S. to create points for harmonization, coordination, and cooperation. The future of transatlantic data trade turns on developing shared understandings of privacy within these new structures.

II. Different Visions of Data Privacy

This Part considers how the two systems of data privacy law, EU and U.S., envision the individual. From the perspective of an anthropologist, law is "a species of social imagination."[17] As Clifford Geertz observes, "legal thought is constructive of social realities" and not merely "reflective of them."[18] 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."[19] This shared cultural background forms a key part of juridical decision-making. He notes, "In this mental background every problem finds its setting."[20]

---

[14] *See infra* Section II.B.
[15] *See infra* Section II.C.
[16] JÜRGEN HABERMAS, ZUR VERFASSUNG EUROPAS 66 (2011).
[17] CLIFFORD GEERTZ, LOCAL KNOWLEDGE: FURTHER ESSAYS IN INTERPRETIVE ANTHROPOLOGY 232 (1983).
[18] *Id.*
[19] BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 12 (1921).
[20] *Id.* at 13.

This Part examines how two legal orders construct contrasting "legal identities" for individuals as bearer of data privacy interests.[21] To sketch our overall argument regarding the "mental background" of these areas of law, we find 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. In the U.S., in contrast, the 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. As a consequence 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 U.S.'s privacy consumer across three dimensions: (1) her constitutional protections; (2) her statutory protections; and (3) and her relative legal status compared to the entities that collect and process her personal data. Part II.A and Part II.B *infra* examine the respective visions in the EU and U.S. for the individual as rights-bearer.

Before we begin, some brief points about terminology and scope would be helpful. This Article adopts the respective terminology of each legal system in identifying 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."[22] When we desire a neutral term, this Article refers to "data privacy law."[23] We now turn to the different models of the individual as rights-bearer in the two systems.

A. "Rights Talk" in the EU

This Article uses the term "data subject" to refer to the rights-bearer in the EU's data protection law. A feature of the EU is its "multi-linguism." All its official documents are translated into the twenty-four languages of the Member States, and all versions are of equal legitimacy.[24] In English Euro-speak, EU data protection law uniformly calls the individual whose data are processed the "data subject," and we therefore adopt this term.[25] Linguistics also teaches us that the subject is the most prominent active agent of a sentence. In a similar fashion, the EU privileges the prominence of the individual whose personal information is processed. It engages in a rights-focused legal discourse centered on the data subjects.

---

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

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

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

[24] For a discussion of multi-lingualism in data protection law, see GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 9 (2014).

[25] *See, e.g.*, DP Directive, *supra* note 6, at 33; GDPR, *supra* note 7, at 2.

1. Constitutional Protections and "Rights Talk." 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 post-war constitutions of Italy (1947) and Germany (1949) were in the front ranks of this development.[26] 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 post-war identity, Europeans also developed a supranational system of fundamental rights. These interests are now protected by institutions both within the European Union, such as the European Court of Justice, and outside of it, such as the European Court of Human Rights.

The trend of supra-national rights in the post-war European order extends the already significant role of "constitutional politics" within European nations. 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.[27] The European Convention of Human Rights and the Charter of Fundamental Rights function as the two pillars of fundamental rights in Europe. As Frederico Fabbrini summarizes, there is a "plurality of constitutional sources enshrining constitutional rights" and a "plurality of constitutional views on human rights."[28] There is also a plurality of judicial bodies, national and transnational, involved in interpreting, enhancing and extended these different sources. 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 (1950) 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."[29] The Convention established the European Court of Human Rights, which has built on Article 8 to identify specific rights regarding data protection.

Within the EU, the key constitutional document is the Charter of Fundamental Rights (2000). With the signing of the Lisbon treaty by EU Member States, the Charter became binding constitutional law for the EU in 2009.[30] 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."[31] The Charter protects privacy, like the Convention, and also contains an explicit right

---

[26] GRUNDGESETZ [GG] [Basic Law], Art. 1–2, *translation at* https://www.gesetze-im-internet.de/englisch_gg/; Art. 2–3 Constituzione [Const.] (It.).
[27] ALEC STONE SWEET, GOVERNING WITH JUDGES 3 (2000).
[28] FEDERICO FABBRINI, FUNDAMENTAL RIGHTS IN EUROPE 26 (2014).
[29] THE EUROPEAN CONVENTION ON HUMAN RIGHTS art. 8 (1950).
[30] JEAN-CLAUDE PIRIS, THE LISBON TREATY 146 (2010).
[31] *Id.*

to data protection.[32] Article 8(1) provides: "Everyone has the right to the protection of personal data."[33] 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. In Fabbrini's assessment, this overlap of judicial institutions and governance layers for protecting human rights creates "an incentive for expansion of the norms and institutions for the protection of fundamental rights."[34]

These transnational developments have been accompanied by recognition of a constitutional right to data protection in several EU Member States. These include Germany's path-breaking "right to informational self-determination" of 1983 and its "right of trust and integrity in information systems" of 2008.[35] 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.[36] Here is further evidence of Fabbrini's "plurality of constitutional sources enshrining constitutional rights."[37]

As is common in Europe for constitutional rights, moreover, the EU's rights to privacy and data protection do not merely constrain the government. While 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. [38] U.S. constitutional rights are generally limited to only the latter; in American terminology, the threshold requirement is for "state action."

The resulting European data protection system centers itself around the data subject as a bearer of rights. It does so to respond to the dangers of the processing

---

[32] Charter of Fundamental Rights of the European Union, 18 Dec. 2000, art. 8(1), 2000 O.J (C 364) 10 [hereinafter Charter].

[33] *Id.* A right to data protection is also protected by Article 16 of the Treaty on the Functioning of the EU (2008). Treaty on the Functioning of the European Union, 9 May 2008, art. 16, 2008 O.J (C 115) 49 [hereinafter Functioning Treaty].

[34] FABBRINI, supra note 28, 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 finding that EU law protects a "right to respect for private life with regard to the processing of personal data." Cases C-92/09 Schecke and C-93/09 Eifert v. Land Hessen 2010 E.C.R. 662 (Nov. 9, 2010) (establishing this critical combination). Through this language, the Luxembourg Court formally constitutionalizes data protection while also failing to conceptualize the relationship between the Charter's protections for privacy and data protection.

[35] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Decision of Dec. 15, 1983, 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); Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Decision of Feb. 27, 2008, 1 BvR 370/07, 1 BvR 595/07, *translation at*: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

[36] FUSTER, *supra* note 24, at 66–70.

[37] FABBRINI, *supra* note 28, at 26.

[38] Case C-144/04, Mangold v. Helm 2005 Eur. Ct. H.R. 709 (Nov. 22, 2005).

of personal data. As the French national data protection law of 1978 warns, "informatics" poses a danger to "human identity, human rights, privacy, [and] individual or public liberties."[39] 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."[40] 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 integrity."[41] 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."[42]

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: all personal data processing requires a legal basis.[43] Article 8(2) of the EU Charter requires that data be processed only based on a "legitimate basis laid down by law."[44] A processing of 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. In its decision in *Schrems*, the European Court of Justice 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 persons concerned have suffered any adverse consequences on account of that interferences."[45] The same point was made in *Google Spain*, where the European Court of Justice observed that

---

[39] French Data Protection Law, art. 1, *translation at* https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf.

[40] 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.

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

[42] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Decision of Dec. 15, 1983, 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).

[43] NIKO HÄRTING, DATENSCHUTZ-GRUNDVERORDNUNG 80 (2016).

[44] 2012 O.J. (C 326) art. 8. In its decision in *Schrems*, the European Court of Justice found 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).

[45] *Schrems*, *supra* note 9, at ¶ 87.

the data subject's fundamental interests do not turn on whether "the inclusion of the information in question ... causes prejudice to the data subject."[46] Rather, a processing of 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.

As part of this approach, EU law proceeds by first enacting "omnibus laws."[47] 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.[48]

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.[49]

European Law also supplies a definite path to legal protection following harms to the data subject. There is no need for harm to a monetary or property interest when personal information is misused.[50] Both the data subject and a data protection authority can request an injunction to stop a practice that harms a privacy interest and receive damages based on a non-material injury in cases of a serious invasion of one's protected sphere of privacy.[51] Continuing this approach, the GDPR explicitly allows for compensation for both "material or non-material damage" following a failure to fulfill its requirements.[52]

3. Data Subject versus Data Processor. Like other rights in the EU system, data protection is not boundless. Nonetheless, data subjects are granted a privileged position by EU law, 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 freedom."[53] In the first part of Article 52(1), moreover, the Charter requires a legal basis, such as a statutory provision, for limiting a right. The second part of Article 52(1) then creates a guarantee of protection for "the essence," or core, of rights and freedoms.[54] This language means that the core part of each right must

---

[46] Case C-131/12, Google Spain v. AEDP 2014 E.C.R. 317, ¶ 91 (May 13, 2014) [hereinafter Google Spain].
[47] For a discussion, see SOLOVE & SCHWARTZ, Casebook, *supra* note 23, at 1096.
[48] *Id.*
[49] Paul M. Schwartz, *The EU-U.S. Privacy Collision*, 126 HARV. L. REV. 1966, 1976-77 (2013).
[50] JAN PHILIPP ALBRECHT & FLORIAN JOTZO, DAS NEUE DATENSCHUTZRECHT DER EU 126–29 (2017).
[51] BGHZ 128, 1, 15- Caroline von Monaco (1995).
[52] GDPR, *supra* note 7, at art. 82(1).
[53] Charter, *supra* note 32 at art. 52(1).
[54] *Id.*

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.

To be sure, EU law protects 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 this goal in 1995.[55] The attempt to ensure high standards of data protection in all Member States forms part of this protection of "free flow of personal data." 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 individual with regard to the processing of such data must be equivalent in all Member States."[56] 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."[57] There is also recognition here of the monetary value of international flows of information.

Beyond the directive, treaties of the European Union 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.[58] Outside of its data protection policy framework, the EU's interest in free flow of information forms part of its landmark legal initiative to create a digital single market in the EU.[59] Other interests recognized by EU law that can conflict with data protection include a right to access information, freedom of expression, and journalistic freedoms. The Charter of Fundamental Rights protects these interests in its Article 11.[60]

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 post-war European constitutional law. He depicts it as consisting of a "least means test."[61] The idea is that "it is never constitutionally sufficient ... that the constitutional benefits outweigh the constitutional costs; instead the benefits must be achieved at the least constitutional costs (least means)."[62] The European Charter of Fundamental Rights adopts the proportionality test for restrictions on any of its fundamental interests in its Article 52(1).[63] In the EU's proportionality analysis, there is no privileging of information flow and of the other

---

[55] DP Directive, *supra* note 6, at Recital 3.

[56] *Id.* at Recital 6.

[57] *Id.* at Recital 8.

[58] *See* Functioning Treaty, *supra* note 34. 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 7, at art. 1.

[59] EUROPEAN COMMISSION, DIGITAL SINGLE MARKET, https://ec.europa.eu/priorities/digital-single-market_en (last visited Jan. 30, 2017).

[60] Charter, *supra* note 32, at art. 11.

[61] SWEET, *supra* note 27, at 98.

[62] *Id.*

[63] *See* Charter, *supra* note 32, at art. 52(1). For use of this test in a privacy case, see Case C-291/12, Schwarz v. Bochum, 2013 E.C.R. 401 (June 13, 2013).

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.[64]

Taken as a whole, data protection law does not concern itself greatly with how its protection of the data subject might impact negatively on useful activities of data processors.[65] 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, an interference with "the fundamental rights to privacy and to the protection of data" cannot "be justified by merely the economic interest which the operator of such an engine has in that processing."[66] 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.

B. "Marketplace Discourse" in the U.S.

In referring to the individual whose personal data are processed, many U.S. privacy laws use the term "consumer" [67] or identify the individual based on a specific consumer relationship. Other laws identify the individual based on a specific consumer-relationship.[68]

These statutes all situate the individual squarely in marketplace relations, whether as a consumer, customer, or as a "subscriber" of telecommunications. In a nod to this dominant language, this Article refers to a bearer of privacy interests in the U.S. as the "privacy consumer." 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 one can maximize her preferences regarding data trades. The focus of information privacy law in the U.S. is policing fairness in exchanges of personal data.

1. Constitutional Protections. Our analysis begins with the private sector. There is no constitutional right to information privacy in the U.S. analogous to the EU's right to data protection. The U.S. Constitution generally does not extend to

---

[64] SWEET, *supra* note 27, at 98–99.

[65] Thus, the General Data Protection Regulation 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 7, at Recital 6. But it does so within the context of the requirements for a need 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.

[66] Google Spain, *supra* note 46, at ¶ 81.

[67] Such laws include the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Video Privacy Protection Act. *See* 15 U.S.C. § 1681 (Fair Credit Reporting Act); 15 U.S.C. §§ 6801–6809 (Gramm-Leach-Bliley Act); 18 U.S.C. § 2710 (Video Privacy Protection Act).

[68] For example, the Cable Act speaks of "subscribers," and the Telecommunications Act of "customers." *See* 47 U.S.C. § 631 (Cable Act); 47 U.S.C. § 222 (Telecommunications Act).

"horizontal-to-horizontal," or private, relations that are purely among private individuals.[69] Moreover, the Constitution does not oblige the government to take positive steps to create conditions to allow the existence of fundamental rights.[70]

In the public sector, there is only a limited interest in information privacy in the U.S. 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 by the government of personal information. It safeguards a right of the people to be secure against searches of "persons, houses, papers and effects."[71] 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.[72] Under the caselaw of the Supreme Court, moreover, the Constitutional does not protect the individual when a "third party," such as her bank, surrenders her personal information to the government.[73] 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* (1977) to identify a general right to "information privacy."[74] Almost four decades after the Supreme Court articulated the *Whalen* interest, both its very existence and its reach remain uncertain.[75] At least one court has expressed "grave doubts" about whether this interest is no more than mere dicta from the 1977 decision.[76] In its most recent case concerning the right to informational privacy the Supreme Court proved unwilling to resolve doubts concerning this right's viability. In *NASA v. Nelson*, in ruling against the plaintiff, the Supreme Court stated that it

---

[69] *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).

[70] Deshaney v. Winnebago Cty. Dep't of Soc. Servs., 489 U.S. 189 (1989).

[71] U.S. CONST. amend. IV.

[72] This idea could be called the "first party" doctrine as opposed to the "third party doctrine." Smith v. Maryland, 442 U.S. 735 (1979), 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 seen in the context of data mining. *See* Paul M. Schwartz, *Regulating Data Mining in the United States and German*, 53 WM & MARY L.REV. 351, 356 (2011).

[73] Smith v. Maryland, 442 U.S. 735 (1979).

[74] 429 U.S. 589 (1977).

[75] 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*, 80 IOWA L. REVIEW 553, 574–82 (1995).

[76] 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 found that the right to information privacy protects only a small set of rights that can be deemed "fundamental." J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981).

merely assumed the existence of the *Whalen* right, but "without deciding" the matter.[77] At best, and as developed in case law 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 policy."[78] The resulting constitutional scrutiny by federal courts tends not to be highly demanding.[79] Compared to the EU, the U.S. lacks any analogous right to data protection and information self-determination.[80]

The most significant constitutional safeguards for information in the U.S. concern the free flow of data, and 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* (2011), for example, the Supreme Court invalidated a Vermont law that prevented pharmacies from selling prescriber-identifying information without the consent of the prescribing party.[81] 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."[82] The First Amendment is likely to be an increasingly fertile source of rights for data processors in other areas of the economy. For example, Chris Hoofnagle warns that the Fair Credit Reporting Act, 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.[83]

Constitutional requirements for standing in the U.S. provide another source of protection for data processors. Without concrete harm, there is no "case or controversy" under Article III that would permit recourse to the judicial system. 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"[84] The law in the U.S. remains uncertain about whether a variety of information processing 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

---

[77] NASA v. Nelson, 562 U.S. 134, 163 (2011).

[78] United States v. Westinghouse Elec. Corp., 638 F.2d 570, 579 (3d Cir. 1980). Of the cases recognizing a *Whalen* interest, the Third Circuit decision in *Westinghouse* has been the most influential.

[79] *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 N.Y., 712 F.2d 1554, 1559 (2d Cir. 1983); State v. Russo, 790 A.2d 1132, 1147–50 (Conn. 2002). For an overview of the caselaw, see SOLOVE & SCHWARTZ, *supra* note 23, at 565–81.

[80] Schwartz, *supra* note 75, at 381-87.

[81] 564 U.S. 552 (2011).

[82] *Id.* at 557.

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

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

privacy statute allowed actions for violation of its provisions and provided liquidated damages for recovery.[85] By an 8-2 vote, the Court declared that notwithstanding a statutory violation in the case before it as well as a statutory recovery mechanism through liquidated damages, Article III required a plaintiff to demonstrate an "injury in fact" that needed to be "concrete and particularized."[86] This constitutionalization of privacy harms represents an invitation to federal courts to rewrite and narrow the privacy statutes that allow statutory damages.[87]

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 takes action, 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. Regulatory action also frequently requires a "horror story," that is, convincing evidence of abusive data practices.[88]

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 F.T.C. has detailed the practices of "data brokers" and how this industry circulates its information with scant transparency and free of legal oversight.[89] As its 2014 Report on this industry stated, "Data brokers collect data from numerous sources, largely without consumers' knowledge."[90]

Where the EU views its laws as reflecting and making concrete the broader mandates of a fundamental privacy right, the U.S. anchors its information privacy law in the marketplace. Market discourse and its logic are dominant. As an illustration, the mission of the Federal Trade Commission (FTC), the long established "privacy cop" in the U.S., is "to protect consumers and promote competition."[91] It acts to prevent "unfair or deceptive acts or practices in or affecting commerce."[92] Another agency, the Federal Communications Commission (FCC), has taken on a new prominence in the policy arena for information privacy. Its current focus is on protecting consumers in their relations with ISP's, formally termed "broadband Internet access services."[93] For the FCC, too, the language of privacy protection is that of the market, or more specifically, the specific market for

---

[85] 136 S.Ct. 1540, 1550 (2016).

[86] *Id.* On the origins of this test, see Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. Inc., 528 U.S. 167, 180–81 (2000); Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992).

[87] For a summary of these statutes, see SOLOVE & SCHWARTZ, *supra* note 23, at 194–96.

[88] On the importance of such "outside events" opening a "policy window" for privacy, see PRISCILLA M. REGAN, LEGISLATING PRIVACY 199 (1995).

[89] FTC, DATA BROKERS (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[90] *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.

[91] *What We Do*, FTC, https://www.ftc.gov/about-ftc/what-we-do (last visited Jan. 30, 2017).

[92] 15 U.S.C. § 45(a)(1).

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

broadband networks.[94] 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.[95]

The White House provides final examples of marketplace discourse around privacy. Its 2012 Report, *Consumer Data Privacy in a Networked World*, focuses on the role of "consumers' trust in the technologies and companies that drive the digital economy."[96] In it, the White House notes the positive role of data trade and the governmental role in "promoting innovation."[97] The report emphasizes how: "personal data fuels an advertising marketplace that brings many online services and sources of content to consumers for free."[98]

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 U.S., in contrast, the strongest constitutional protections are not for the individuals whose data are at stake, but data processors. There is no equivalent in the U.S. to the EU's right to data protection. Furthermore, there is no constitutional requirement in the U.S. that data processors have a legal basis for any use of personal data.

In the tug-of-war between individuals and data processors, moreover, information privacy law in the U.S. 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.[99] 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 administration of President Bill Clinton. First and foremost, the American approach has sought to create a regulatory environment to promote the growth of technology companies.[100] As part of this inclination, there has been a long reliance on industry self-regulation. The early importance of this aim was established by an influential 1997 Commerce Department compilation of papers regarding industry self-regulation of privacy in the information age.[101]

---

[94] *Id.*

[95] *See infra* Section IV.A.

[96] CONSUMER DATA PRIVACY, *supra* note 12, at 1.

[97] *Id.*

[98] *Id.* at 5.

[99] 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 U.S. EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK 62 (2013).

[100] For a discussion, for example, 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).

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

Solicitude for the supply-side continues to be a central part of the U.S. privacy landscape. As noted, the Obama White House sought to further consumer trust "while promoting innovation."[102] Its goal is for this policy to spread globally; the White House hopes that U.S. leadership in "consumer data privacy can help establish more flexible, innovation-enhancing privacy models among our international partners."[103] The FCC, the newest "privacy cop" in the U.S., provides a further example of such concern for the health of the data marketplace. Its 2016 Notice of Proposed Rulemaking (NPRM) emphasized its support "for the ability of broadband networks to be able to provide personalized services, including advertising to consumers – while reaping the financial rewards therefrom."[104] In its NPRM, the FCC also emphasized the need for "continued broadband investment and deployment."[105]

C. Shared Doctrine: Contract and Consent

The previous two sections have identified the profoundly different visions of the individual as rights bearer in EU and U.S. data privacy law. Yet, a potential future basis for greater interoperability of the EU and U.S. law of international data transfers might be around notions of consent and contract. After all, a legal system's tool kit of available doctrines and concepts influences how it resolves social conflicts and problems. The point has been summed up in vernacular wisdom as the "Law of the Instrument," which holds: "If all you have is a hammer, everything looks like a nail." At a general level, the U.S. and EU Member States have similar "hammers." This section explores similarities in these consensual doctrines and the U.S. and EU.

In the U.S. and EU alike, contract and consent promote individual self-determination. Whether in the U.S. or on the continent, a contract is a way to mark a binding promise. As Alan Farnsworth summarizes regarding the U.S., a contract makes enforceable an exchange of promises.[106] In the continental tradition, there is a similar notion that a contract is an agreement that creates a legal obligation. In EU law, moreover, "freedom of choice" is regarded as a fundamental principle.[107] European law grants parties the free choice to regulate the content of a contract. Such freedom exists, for example, regarding choice-of-law questions. As the Rome I Regulation states, "A contract shall be governed by the law chosen by the parties."[108]

Beyond contract, similarities abound in Europe and the U.S. regarding consent. In the U.S. and on the continent, it has a double role. Consent is a concept both within contract law and outside it. As part of contract, it represents a preliminary step to forming a binding agreement. Consent of the parties is an indication of a party's will, usually a necessary one, for entering into a legal relationship. Outside of the setting of contract law, consent represents a manifestation of one party's agreement. It plays an especially important role in tort

---

[102] *See* CONSUMER DATA PRIVACY, *supra* note 12, at 1.
[103] *Id.* at 5.
[104] FCC, Notice of Proposed Rulemaking 2500, 2506 FCC 16-39 (April 1, 2016).
[105] *Id.*
[106] ALLAN FARNSWORTH, CONTRACTS 3-4 (2d ed. 1990).
[107] Jürgen Basedow, *Freedom of Contract in the European Union*, 6 EUR. REV. PRIVATE L. 901 (2008).
[108] 2008 O.J. (L 177) art. 3.

law in Europe and the U.S. For example, legal systems in Europe and the U.S. rely on consent in the medical setting as a way to protect a right to one's bodily integrity.[109] Informed consent obviates the basis for an action for battery due to an impermissible physical contact. Informed consent to medical treatment does not, however, imply consent to a contract; for example, it does not settle the terms for the doctor's payment.

Consent also plays an important role in tort law where it waives certain possible claims. As a general matter, an individual can manifest her free will by consenting to an otherwise injurious act. Both the common law and civil law have adopted the proverb attributed to the Roman jurist Ulpian: *Volenti non fit iniuria*. "To a willing person, injury is not done."[110] The person who proffers consent to a battery, for example, has no action in tort.[111]

There is also a link here with tort privacy, where in the U.S. and EU alike, consent can negate an otherwise tortious invasion of privacy. In his famous article, *Privacy* (1960), Dean William Prosser lists "consent to the invasion" as "[c]hief among the available defenses" to his four privacy torts.[112] In a canonical tort privacy case from 1953, *Gill v. Hearst,* the California Supreme Court decided that a couple embracing in a public setting had implicitly consented to be photographed.[113] Through "their own voluntary action," the two had "waived their right of privacy so far as this particular public pose."[114] In Europe, consent also plays an important role in tort privacy. For example, European caselaw similar to *Gill v. Hearst* explores when one's presence in a public area amounts to implicit consent to being photographed. Notable cases concerning this issue exist at the national level and before the European Court of Human Rights.[115]

---

[109] The leading cases in developing informed consent in the U.S. are Canterbury v. Spence, 464 F.2d 772 (D.C. Cir. 1972) and Schloendorff v. Society of N.Y. Hospital, 105 N.E. 92 (N.Y. 1914). In Germany, this principle is codified in the Civil Code at BGB § 630d. Bürgerliches Gesetzbuch [BGB] [Civil Code], BGBl. I S. 42, ber. S. 2909 and BGBl. 2003 I S. 738, § 630d *translation* at https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p2651. German Criminal Law has also adopted this concept in the Criminal Code. Strafgesetzbuch [StGB] [Penal Code], StGB § 228.

[110] For a discussion of the doctrine in modern U.S. tort law, see RICHARD EPSTEIN & CATHERINE M. SHARKEY, CASES AND MATERIALS ON TORTS 14–27 (11th ed. 2016). For the German use of this doctrine, see ANSGAR OHLY, "VOLENTI NON FIT INIURIA" - DIE EINWILLIGUNG IM PRIVATRECHT 21 (2002). On its incorporation into the German Criminal Code, see Strafgesetzbuch [StGB] [Penal Code], § 228 StGB.

[111] OHLY, *supra* note 110 at 22–27; *see also*, BASIL S. MARKESINIS & HANNES UNBERATH, THE GERMAN LAW OF TORTS 80 (4th ed. 2002).

[112] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 419 (1960). He also observed that such consent might be express or implicit, as "by conduct, such as posing for a picture with knowledge of the purposes for which it is to be used, or industriously seeking publicity of the same kind." *Id.* at 419–20.

[113] Gill v. Hearst, 253 P.2d 441 (Cal. 1953).

[114] *Id.* at 443.

[115] For German cases, see Federal Constitutional Court, 63 NJW 1587, at para. 24 (2010); Federal Constitutional Court, BVerfGE 82, 236, 269; Federal Constitutional Court BVerfGE 97, 125, 149 – Caroline von Monaco. For European Court of Human Rights caselaw on this issue, see Case of Von

In sum, contract and consent provide a way to exercise individual self-determination in both the U.S. and on the continent. The law in both the U.S. and Europe has also wrestled with when and how to limit decision-making through these mechanisms. In consenting, a person exercises self-determination even if agreeing to a harm to an interest. As Marion Baston-Vogt observes, such agreement represents "use of his own right of self-determination through a particular expression of will."[116] At the same time, however, certain kinds of bad contracts and bad choices degrade personhood; hence, the question becomes the extent to which the law should prohibit or otherwise restrict such decisions.

In the U.S., limits are set on contracts through means such as prohibitions on "contracts of adhesion" and, more generally, through the doctrine of unconscionability.[117] As for consensual mechanisms outside of the contractual setting, U.S. law provides similar protections against certain bad choices. For example, U.S. courts will void consent forms that release recreational facilities from liability resulting from their negligence.[118] Similar to the U.S., the continental tradition both values and limits freedom of contract and consent. During the last half-century, a decisive movement built protections against many types of unfairness into the framework of contract law. Within the continental traditional, German law has distinguished itself through its attention to the fairness of standard terms. This focus, beginning first in the courts, shifted to the legislature with the enactment of the 1977 Act for the Control of the General Conditions of Business (*Allgemeine Geschäftsbedingungen Gesetz*, AGBG).[119]

As a shared starting point then, the two legal systems generally use contract and consent in a similar fashion. This Article now turns to the use made of these consensual mechanisms by EU and U.S. data privacy law. How are these "hammers" used by the different systems? Surprisingly, both systems make only

---

Hannover v. Germany (No. 3) no 8772/10, ECHR 836 (Sept 19, 2013); Case of Von Hannover v. Germany (No. 40660/08 & 60641/08, ECHR 228 (Feb. 7, 2012).

116 MARION BASTON-VOGT, DER SACHLICHE SCHUTZBEREICH DES ZIVILRECHTLICHEN ALLGEMEINEN PERSÖNLICHKEITSRECHT 26 (1997).

117 The former are, in Friedrich Kessler's famous formulation, "[s]tandard contracts ... typically used by enterprises with strong bargaining power" and require legal action against the "abuse of freedom of contract." Friedrich Kessler, *Contracts of Adhesion – Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 632, 641 (1943). As for the latter, unconscionability, the Uniform Commercial Code grants American courts considerable leeway to stop "any unconscionable result." U.C.C. § 2-302 (AM. LAW INST. & UNIF. LAW COMM'N 1977).

118 At first, legal limits were placed only on unfairness in consent when the agreement involved access to essential public services. Thus, U.S. courts invalidated signed releases to negligent injuries when the "party seeking exculpation is engaged in performing a service of great importance to the public." Tunkl v. Regents of Univ. of Cal., 383 P.2d 441 (Cal. 1963). Later courts limited such waivers even when the service involved was not an essential service, such as public transportation, but merely recreational activity on private land. As an example, the Vermont Supreme Court in 1995 voided a pre-injury release signed by a skier that released a ski resort from all liability resulting from its negligence. Dalury v. S-K-I, Ltd., 670 A.2d 795 (Vt. 1995).

119 Bürgerliches Gesetzbuch [BGB] [Civil Code], BGBl. I S. 42, ber. S. 2909 and BGBl. 2003 I S. 738, §§ 305ff.; Graf v. Westphalen, *AGB-Recht im Jahr 2014*, NEUE JURISTICHE WOCHENSCHRIFT [NJW] 2223 (2015).

limited recourse to these consensual mechanisms. Also surprisingly, they do so for different reasons.

III. The European Union: Rights Talk in Action

The question for the next two Parts of this Article is how the EU and U.S. draw on concepts of contract and consent in their respective laws of data privacy. As we have seen in the last section, both systems feature these doctrines. This similarity appears to be promising for the future interoperability of the two legal systems and for resolution of the current transatlantic data war. The next two Parts demonstrate, however, that E.U. and U.S. utilize these consensual mechanisms differently in promoting the interests of their respective data subjects and privacy consumers.

Our main reference for European data protection law is the General Data Protection Regulation (GDPR) of 2016.[120] We also make references to the document that the GDPR will replace, the European Data Protection Directive of 1995.[121] The GDPR takes effect on May 25, 2018, which will mark a decisive moment for international privacy law.[122] As Jan Albrecht and Florian Jotzo observe, the GDPR will on that date "represent without any doubt the most important legal source for data protection."[123] As proof of this significance, Albrecht and Jotzo point to the Regulation's central role in "the largest domestic market in the world," the EU, as well as its future international impact.[124] Albrecht is in a good position to comment on the GDPR; a member of the Green party, he served for the EU Parliament as the influential Rapporteur of the Regulation.[125]

The decision to replace a Data Protection Directive with a Regulation itself demonstrates the rising significance of information privacy. 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.[126] 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.[127] 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, cornerstone documents of European integration safeguard privacy and data protection as human rights. In a reflection of the data subject's high status, the GDPR provides directly binding statutory protection in EU law for her. This choice

---

120 GDPR, *supra* note 7.

121 DP Directive, *supra* note 6.

122 GDPR, supra note 7, at art. 99.

123 ALBRECHT & JOTZO, *supra* note 50, at 7.

124 *Id.*

125 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.

126 Schwartz, *supra* note 49, at 1971–72.

127 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.

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.[128]

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, as we have seen, uses them to further individual self-determination. In its data protection law, however, the EU takes a collective approach to these doctrines.[129] 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 the definition of Susan Rose-Ackerman, an inalienability is "any restriction on the transferability, ownership, or use of an entitlement."[130] 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.[131] 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 non-contract and non-consent.[132] EU data protection law establishes important areas of inalienable privacy. In particular, it sets out bedrock data protection principles that are not subject to individual waiver and cannot be traded away in bargained-for exchanges.[133] Some of these restrictions are embedded at the constitutional level, others at the statutory level.

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 EU Charter of Fundamental Rights states, personal data processing requires "a legitimate basis laid down by law."[134] 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."[135] Such legislation is constructed with the building blocks of Fair Information Practices.[136] These principles express duties and responsibilities for

---

[128] The approach of these Directive has been termed one of "minimum harmonization." STEPHEN WEATHERILL, EU CONSUMER LAW AND POLICY 317 (2d ed. 2013).

[129] 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.

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

[131] Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269 (2005); Schwartz, *supra* note 100, at 2095–13.

[132] Schwartz, *supra* note 100, at 2095–100.

[133] *See, e.g.,* ALBRECHT & JOTZO, *supra* note 50, at 72 (noting core protections in data protection law that the individual cannot "sell" or exchange).

[134] 2012 O.J. (C 326), art. 8.

[135] Shrems, *supra* note, at ¶91.

[136] Schwartz, *supra* note 49, at 1976.

entities that process personal data, and describe rights that people should have regarding the use of their personal information.[137] 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.[138]

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.[139] 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 non-waivable core of safeguards. The GDPR's key expression in this regard is its Article 6.[140] 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.[141]

The list of key principles in the GDPR's Article 6 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).[142] 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.[143] Finally, in Article 51, the GDPR contains strong protections for (9) independent data protection authorities.[144]

---

[137] *Id.*
[138] ALBRECHT & JOTZO, *supra* note 50, at 72.
[139] 2012 O.J. (C 326), art. 8.
[140] 2016 O.J. (L 119), art. 6.
[141] 1995 O.J. (L 281), art. 7.
[142] 2016 O.J. (L 119), art. 6.
[143] *Id.*
[144] *Id.* art. 51.

Regarding inalienabilities, there is no "freedom" of consent or contract that trumps the GDPR's fundamental rules. In the example of Niko Härting, "Even if consent makes data processing legimate," the "data minimization" principle of Article 6 "may make it unlawful."[145] 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."[146] 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 program."[147]

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 goal is to serve and protect the rights of the individual. The Charter grants the European Court of Justice, as ultimate interpreter of European Union law, a central role in developing the rights to privacy and data protection law. The Charter also explicitly protects data protection authorities and assigns constitutional rank to their independent status. It spells out their general tasks, which, in turn, grants them constitutional authority when executing them. The European Court of Justice has already developed an important caselaw devoted to the constitutional elements of independence for data protection authorities.[148]

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," 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."[149] It sets out the powers of and duties for these authorities in considerable detail and requires them to exercise them "impartially, fairly and within a reasonable time."[150] Finally, the GDPR establishes a new European Data Protection Board, which is to coordinate actions among national commissioners and resolve disputes among them.[151]

---

[145] HÄRTING, *supra* note 43, at 26.

[146] CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW 242 (2d ed. 2007) (emphasis removed).

[147] *Id.*

[148] 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." 2016 O.J. (L 119), 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. Schrems, *supra* note 9.

[149] 2016 O.J. (L 119), art. 52.

[150] *Id.* at Recital 129.

[151] *Id.* at ¶ 68.

B. Contract and Consent

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 its Article 6(b), the GDPR explicitly includes contractual agreements as a basis for lawful use of personal data.[152] 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."[153] 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." According to this principle, information cannot be "further processed in a manner incompatible with" the original purpose of collection.[154] Use of information beyond that which is necessary for the contract is impermissible.

EU data protection law has long limited data contracts through these requirements of "necessity" and the "purpose limitation." These restrictions 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.[155] 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."[156] 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."[157]

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

---

[152] *Id.* at art. 6.
[153] *Id.*
[154] Manfred Monreal, *Weiterverarbeitung nach einer Zweckänderung in der DS-GVO*, ZEITSCHRIFT FÜR DATENSCHUTZ 250, 252 (2016).
[155] Ulrich Dammann, *Erfolge und Defizite der EU-Datenschutzgrundverordnung* 307, 311 ZEITSCHRIFT FÜR DATENSCHUTZ (2016).
[156] 2016 O.J. (L 119), art. 7.
[157] Dammann, *supra* note 155, at 311.

list" of unfair terms.[158] 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 under the contract, to the detriment of the consumer."[159] 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."[160]

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 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. As a result, consent proves a far less attractive grounds 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."[161] 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." 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.[162] Where consent involves the personal data of a child or sensitive data, there are additional enumerated conditions that must be met.[163] Finally, the burden of demonstrating consent is placed squarely on the data processor, who, in data protection terminology, is called "the controller."[164]

In sum, the GDPR reflects a restrictive view of consent, and 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.[165] He recommends that companies "reduce their reliance on consent as a legal

---

158 2016 O.J. (L 119), ¶ 42.

159 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. Lawyer 6, 9 (2006) (analyzing the Unfair Terms Directive and its "non-exclusive list of terms that may be deemed unfair.").

160 GDPR, *supra* note 7, at Recital 42.

161 *Id.* at art. 4.

162 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; all of these steps must be fulfilled for consent to be legally valid. These requirements are that (1) consent must be a clear and unambiguous indication of wishes; (2) consent must be freely given; (3) consent must be specific; and (4) consent must be informed. Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 01197/11/EN (WP187) 35 (2011).

163 GDPR, *supra* note 7, at art. 8(1).

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

165 KUNER, *supra* note 146, at 68.

basis for data processing to situations where it is absolutely necessary."[166] Kuner's recommendation from 2007 was based on his reading of the Directive, and similar advice regarding a limited use of consent is merited as well under the GDPR.

IV. The United States: Protecting the Privacy Consumer

U.S. privacy law situates the consumer within a marketplace for data trade. This orientation marks a considerable distance from the EU's rights discourse about its data subjects. EU law also takes certain rights and interests "off the table" for consent and contract. Through the Charter, the Directive, and now the GDPR, it safeguards a broad group of binding inalienable principles. In contrast, U.S. law uses the FTC to police data exchanges against the most deceptive kinds of practices. There are equally important differences between the U.S. and EU regarding the comparative constitutional aspects of information privacy law and data protection law, and the incorporation of doctrines of contract and consent.

A. Policing the Marketplace: Statutes and the FTC

In contrast to the EU, U.S. law makes scant use of information privacy inalienabilities. At the statutory level, the most important inalienabilities concern mandated disclosure and notice regarding privacy practices. In the U.S., the FTC makes the most important use of a privacy inalienability. It does so through its "notice-and-consent" enforcement approach. Unlike the EU's inalienabilities constructed through broadly-written and mandatory FIPs, the FTC proceeds through construction of a legal fiction regarding the consent of an idealized consumer.

1. Statutes. In the U.S., 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-Sharar and Carl Schneider observe, "[D]isclosures were mandated almost wherever we looked."[167] 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."[168]

U.S. privacy law is a great believer in 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. The Gramm-Leach-Bliley Act is a leading example

---

[166] *Id.*

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

[168] *Id.* at ix.

of such a federal law; it requires financial institutions to supply consumers with notices that explain these companies' privacy practices.[169] 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."[170]

Another area of mandated disclosure concerns data breach notifications, which are required by forty-seven states and for covered health care information by the federal HITECH Act.[171] State law has also imposed notification requirements beyond data breach notification. In California, for example, all commercial websites must post a privacy policy if they collect personal information from their visitors.[172] California also requires financial privacy disclosures with slightly different content than that under the Gramm-Leach-Bliley Act; as a consequence, Californians receive two types of notices, with almost complete overlap, from their financial institutions.[173]

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."[174]

2. Consent as Fiction. In the U.S., the FTC draws on Section 5 of its organic act, the Federal Trade Commission Act of 1914, 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 its organic act.[175] Second, and as a more pervasive restriction, the FTC can act under Section 5 only to prevent "unfair or deceptive acts or practices in or affecting commerce."[176]

In stopping unfair or deceptive commercial behavior, the FTC acts against practices that precede consensual agreement and are independent of contractualism. In its enforcement actions in the informational privacy context, moreover, the FTC

---

169 15 U.S.C. § 6803.

170 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.

171 For a summary chart of the state data breach notification statutes, see DANIEL SOLOVE & PAUL SCHWARTZ, PRIVACY LAW FUNDAMENTALS 207–09 (4th ed., 2017). 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.

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

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

174 SHAHAR & SCHNEIDER, *supra* note 167, at 10.

175 15 U.S.C. § 46. 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).

176 15 U.S.C. § 45.

has favored use of 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."[177] The core group of the FTC's deceptive enforcement actions rests on its theory of "notice-and-consent."[178]

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 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.[179] 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."[180]

In the uncertain privacy landscape of the U.S., the FTC has stopped companies from tricking consumers, over-promising privacy, and engaging in unexpected and unreasonable data practices. Yet, its connection between deception and consent rests 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."[181] The FTC's assumed premise is that an imagined consumer actually read a privacy statement and agreed to the terms in it-- and to these terms alone. The deceptive merchant then flouted this idealized individual's consent. In reality, consumers generally do not read privacy policies and are unaware of company's data policies. As an aphorism among privacy professionals holds: "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 through by a collective enforcement strategy of the type that EU data protection law carries out on a far greater scale.

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

---

[177] FTC Policy Statement on Deception, 103 F.T.C 174 (1983).

[178] For an evaluation of the FTC's notice-and-consent jurisprudence, see Solove & Hartzog, *supra* note 175, at 636–38; HOOFNAGLE, *supra* note 83, at 365.

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

[180] Solove & Hartzog, *supra* note 175, 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 83, at 160.

[181] LON L. FULLER, LEGAL FICTIONS 51 (1967).

mechanism. The U.S. approach to contracts is one largely favorable to letting parties reach agreement on their own terms.[182] Yet, contract proves largely irrelevant to information privacy law in the U.S. 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 non-binding 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; as a consequence, 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 as a consequence 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 or not such privacy policies or notices constitute a contract. Some courts have found that these statements are per se unenforceable in contract; other courts have found that they might be contracts, but tend then to rule that 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 non-binding statement of policy. As an example, plaintiffs in a class action lawsuit alleged in 2005 that Northwest violated a contractual promise that information it collected would be used only for limited purposes.[183] The airline had, in fact, shared extensive consumer data with a federal agency to assist in its study of airline security.[184] For the *Northwest* court, however, the Airline's promises were only "general statements of policy."[185] It concluded that the privacy notice posted on the airline's website did not constitute a contractual agreement with the company's customers.[186]

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*[187] and *In re American Airlines Inc. Privacy Litigation*.[188]

---

[182] 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).

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

[184] *Id.* at *5.

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

[186] 2004 WL 1278459, at *6.

[187] 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

[188] 370 F. Supp. 2d 552, 554 (N.D. Tex. 2005).

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.[189] The Restatement of Consumer Contracts, now in the drafting process, contains a thorough survey of the current case law and finds, "While 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."[190] 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 or not the future leads to courts reading privacy policies as contracts.[191] Contract law in the U.S. will play a modest role in information privacy law and do little to protect privacy consumers.

2. Consent. In the U.S., 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 U.S. does make use of consent, however, and 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. 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 Fair Credit Reporting Act (FCRA) contains one of the strongest opt-in mechanisms for consent in U.S. information privacy law.[192] The first federal information privacy law in the U.S., FCRA regulates use of "consumer credit reports" by "consumer reporting agencies."[193] 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." These permissible transfers of data and resulting use by the recipient third party occur without the affected consumer's consent.

---

189 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. Since personal information is, according to this court, not freely tradeable, an alleged misappropriation of it in violation of contract did not harm anyone. *Id.*

190 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.*

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

192 15 U.S.C. §§ 1681–1681x.

193 These entities are popularly called "credit reporting bureaus"; the "big three" are Equifax, Experian, and TransUnion. SOLOVE & SCHWARTZ, *supra* note 23, at 741.

FCRA turns to consent mechanisms, however, when consumer credit reports are to be used for employment purposes,[194] or when they contain medical information.[195] Congress in amendments to FCRA in 1996 viewed these areas as more sensitive than others in which credit reports were used.[196] As a consequence, it sought to involve the consumer by informing her of the planned use and requiring her consent.[197] 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.[198] 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.[199]

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. 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."[200] As they note, "A single disclosure may be manageable, but en masse, disclosures are overwhelming, and people cannot hope to attend to more than a trickle of the flood."[201]

Other uses of opt-in consent are found in the Video Privacy Protection Act (VPPA)[202] and Children's Online Privacy Protection Act (COPPA).[203] The "warning function" of consent in the VPPA regards the sharing of "prerecorded video content."[204] Its scope is restricted, however, to information about title and content of audio visual material. The VPPA permits release of other information about the customer's relationship with the video-providing company. For example, video providers can disclose information that does not include "title, description, or subject matter of" audio visual material.[205]

COPPA requires parental opt-in before a website may collect personal information from any child, which it defines as individuals under age 13.[206] The

---

194 15 U.S.C. § 1681b(b).
195 *Id.* at § 1681b(g).
196 Omnibus Consolidated Appropriations Act of 1997, P.L. 104-108, The Statute at Large, at 110 Stat. 3009-430 (1997).
197 15 U.S.C. § 1681b(b)-(g).
198 *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.*
199 *Id.* § 1681b(g).
200 SHAHAR & SCHNEIDER, *supra* note 167, at 95.
201 *Id.*
202 18 U.S.C. § 2710.
203 15 U.S.C. §§ 6501–6506.
204 18 U.S.C. § 2710(a).
205 *Id.* § 2710(b)(2)(D).
206 5 U.S.C. § 6502.

"warning function" of the requirement of "verifiable parental consent" is diminished, however, by a loophole in COPPA. This law only applies if the operator of a website has knowledge that a child is supplying personal information to it. In a decisive weakening of its protections, COPPA permits self-verification of age by visitors to a website that collects personal information. As Kathryn Montgomery observes, nothing in COPPA prevents "a child from simply lying about her age."[207] This aspect of the statute significantly undercuts COPPA's requirement for parental opt-out.

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 Gramm-Leach-Bliley Act (GLBA) illustrates how effectless this right-of-refusal typically proves. Congress enacted the GLBA largely for purposes other than information privacy; most of the Act serves to repeal the Depression-era Glass Steagel Act in order to permit the creation of large financial "supermarkets" in the U.S. 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.[208] The GLBA's general approach is to permit such information use, 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 "non-affiliated third party."[209] 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."[210] In a critique of this practice in 2002, one of the co-authors of this paper observed: "the GLB leaves the burden on bargaining on the less informed party, the individual consumer."[211]

In sum, opt-out consent in the U.S. 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." [212] 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,

---

[207] KATHRYN MONTGOMERY, GENERATION DIGITAL: POLITICS, COMMERCE, AND CHILDHOOD IN THE AGE OF THE INTERNET, 103 (2009).
[208] 15 U.S.C. §§ 6801–6809.
[209] *Id.* § 6802.
[210] *Id.*
[211] 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).
[212] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013).

use, and disclosure of personal data."[213] U.S. data privacy law views the consumers, however, as innately sovereign.

V. Data Privacy's International Future

This Article has identified a conceptual gulf between the data privacy systems of the EU and U.S. based on the different legal identifies 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.

In the U.S., some consider EU data protection as a form of trade protectionism, or the result of misguided jealousy at successful U.S. Internet companies. Here is how President Barack Obama analyzed European investigations into Facebook and Google, "[O]ftentimes what is portrayed a high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."[214] Similar doubts exist on the EU-side regarding American privacy. Jan Albrecht, the EU Parliament's rapporteur for the GDPR, dismisses data privacy law: "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."[215] In assessing U.S. information privacy, Andreas Börding calls attention to its "structural deficits."

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. Part A *infra* considers the socio-political underpinnings for their respective doctrines of consent and contract. Parts B and C returns to the question of transatlantic data flows. It discusses the demise of the Safe Harbor and assesses the Privacy Shield in light of this Article's models of "rights talk" and "marketplace discourse." Part D concludes with thoughts regarding future convergence or divergence for international data privacy law.

A. Constructing Legal Identities

EU data protection is based on "rights talk." In the U.S., in contrast, information privacy proceeds with a model of the privacy consumer who merits protection against deception and unfairness in the data marketplace. Each approach serves significant goals within each system. We now wish to explore these objectives to further a sympathetic understanding of each legal order.

1. The EU. "Rights talk" forms an essential part of the European project, and one that has become more central over time. As Fabbrini notes, there has been a "growth of a fundamental rights culture in Europe in the last few decades."[216] Data protection law is at the front ranks of this effort. The EU began as an economic

---

[213] *Id.* at 1888.

[214] 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.

[215] JAN PHILIPP ALBRECHT, HANDS OFF OUR DATA! 47 (2015).

[216] FABBRINI, *supra* note 28, at 13.

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 co-operation with the goal of bringing lasting peace to Europe. Meeting this goal led to creation of a supranationational authority, and one with "the power to bind its constituent member States." [217] 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.[218] The ordinary European citizen feels bound to her national government, but is likely to have a more distant relationship to the EU as a sovereign entity. Too often, the EU is considered a distant, inaccessible instittuion. 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."[219] 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 European Union is made up of citizens of the Member States ("We the People") as well as the nations of Europe.[220] Each individual therefore participates in the EU in a double fashion: both as a European citizen and through a role in her home nation.[221] 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."[222] Above all, Habermas stresses the need for construction of a "common public sphere" in which citizens of Europe will engage in democratic deliberation.[223] Rather than as Croatians, Czechs, Frenchmen, or Italians, Europeans are to discuss issues that require transnational solutions in a new shared, deliberative space.

---

[217] PAUL CRAIG & GRAINNE DE BÚRCA, EU LAW: TEXTS, CASES, AND MATERIALS 5 (4th ed. 2008).
[218] *Id.* at 58.
[219] *Id.* at 133.
[220] HABERMAS, *supra* note 16, at 66.
[221] *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).
[222] Charter, *supra* note 32, art. 1.
[223] HABERMAS, *supra* note 16, at 59–61.

This new communicative area, Habermas' "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. To be sure, a more conventional explanation for the EU's interest in privacy and data protection 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 certainly heightened sensitivities towards data protection throughout the EU.[224] But there is also a more forward-looking basis for the protection of data privacy.

Data protection law embodies the project of creating a constitutional basis for a pan-European identity. As one German law professor has stated, Europe is no longer conversing in different languages when it comes to data protection law, but now speaks "European."[225] The European language of data protection is 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. For example, 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 decade of progressive jurisprudential developments in the field of human rights."[226]

2. The U.S. How is one then to understand the U.S. approach? One should begin by noting the weak constitutional status of information privacy in the U.S. As a consequence, an approach in the U.S. based around "rights talk" would be unlikely to gain traction. The U.S. Constitution is one of "negative rights" and has scant reach into private sector activities. 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.

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."[227] Americans trust in a notion of progress tied to technology and

---

[224] 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*, 1925, 1948-49 (2010). For a differing account of these developments, see James Q. Whitman, *Two Western Cultures of Privacy,* 113 YALE L.J. 1151, 1180-89 (2004).

[225] Gerrit Hornung, *Eine Datenschutz-Grundverordnung für Europa?*, ZEITSCHRIFT FÜR DATENSCHUTZ 99 (2012).

[226] 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).

[227] Whitman, *supra* note 21, at 399.

"innovation." The last word is especially cherished by tech gurus in Silicon Valley and policymakers in Washington, D.C.[228] From the start of the Internet's commercialization, it has been associated with benefits to consumer as well as the creation of great wealth for the U.S. economy. As Thomas P. Hughes, a historian of technology, notes, "Technology linked to mass consumption is a modern American hallmark."[229]

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 it has enacted privacy legislation, the federal lawmaker has done so to protect consumers within different information marketplaces. Beyond that, it is unwilling to legislate -- as demonstrated by its rejection of the idea of omnibus privacy legislation as early as 1974.[230] The FTC has acted to stop deceptive trade practices and, to a lesser extent, unfairness in the marketplace. [231] But its notion of deception and unfairness ultimately rest on a notion of consumer detriment, which narrows its vision to market relations.

We have now assessed the basis for each legal systems' reliance on either "rights talk" or "market 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 content, EU data protection law channels and restricts these doctrines. In the U.S., 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.

B. 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 U.S. 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

---

[228] Indeed, in Dave Eggers' novel, THE CIRCLE 2 (2013), the word "innovate" appears emblazoned on a stone in a walkway of the Internet company that rules this novel's dystopian world.

[229] THOMAS P. HUGHES, AMERICAN GENESIS 471 (1989).

[230] For a discussion of this path not taken, see REGAN, *supra* note 88, at 77–79.

[231] On the FTC's preference for the deception prong of the FTC Act over unfairness, see HOOFNAGLE, *supra* note 83, at 132–40.

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 demise.

By the late 1980's, European policymakers realized that their efforts to create strong safeguards for data protection necessitated transborder policies for the data of EU citizens. As a result 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.[232] From the EU perspective, moreover, 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 a transfer of personal data from an EU Member State. Both the Directive (1995) and the GDPR (2016) contain this "adequacy" requirement.[233] In consequence, data transfers from the EU to the U.S. 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 U.S. is not adequate."[234] Yet, with so much valuable data trade between the EU and the U.S., both sides had considerable incentives to find policy solutions to bridge their different legal approaches to data privacy. The most significant first-generation 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 represents a bold policy innovation: it transplants EU data protection concepts into U.S. law in a fashion beyond the willingness of 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. While U.S. companies need 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.[235] 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.

---

[232] For a discussion, see Schwartz, *supra* note 5, at 472.

[233] DP Directive, *supra* note 6, at art. 56; GDPR, *supra* note 7, at art. 45.

[234] Article 29 Working Party, *supra* note 8, at 2.

[235] *See, e.g.*, KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND 65 (2015) (discussing interviews with U.S. corporate privacy officials that showed how some companies default "to the highest common denominator, which ... is Europe.").

Another factor made the Safe Harbor acceptable in the U.S. 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.[236]

Despite grumblings in the EU about the Safe Harbor, this treaty's future success seemed assured for the 21st Century with over 5,000 U.S. companies entering into it. When the Commission and the Commerce Department began to consider improvements in a "Safe Harbor 2.0" in 2012, many in the U.S. expected only tinkering with the accepted formula.[237] 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 U.S. Then on October 6, 2015, the European Court of Justice's opinion in *Schrems v. Data Protection Commissioner* ended any hope of only minor changes to the Safe Harbor.[238] 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. Regarding Snowden's leaks, the Luxembourg Court made clear its constitutional objections to the NSA activities.[239] In its opinion, it singled out for especially strong criticism the NSA's massive suspicionless data dragnets and bulk storage of information.[240] 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.[241] 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 European Union."[242]

---

[236] 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 (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).

[237] 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). Regarding the discussion for a Safe Harbor 2.0, see the pre-Snowden recommendations from the Commission to the U.S. 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).

[238] Schrems, *supra* note 9.

[239] *Id.* at ¶ 28.

[240] *Id.* at ¶ 93.

[241] *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.*

[242] *Id.* at ¶ 73 (emphasis added).

C. 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 "E.U.-U.S. Privacy Shield."[243] 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 Shield.[244]

1. Negotiating Perspectives and Positions. This Article now revisits its respective models of EU and U.S. data privacy. Recall the "Law of the Hammer" and Gertz's concept of law as a form of social imagination.[245] Based on the two discourses about privacy, the EU and U.S. 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."[246]

As for the U.S., the demise of Safe Harbor increased the need for a new agreement to permit free information flow with the EU. With its strong market orientation, the U.S. approached the negotiations favoring open choice for consumers regarding data use and broad access to innovative American data services and products.[247] 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 was able to tug the resulting agreement closer to its fundamental principles. At the same time, the U.S. 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 as oversight mechanisms are deployed. 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

---

[243] *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 [hereinafter *Remarks*].

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

[245] GEERTZ, *supra* note 17, at 232.

[246] *Schrems, supra* note 9, at ¶ 21.

[247] 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 243.

limitation," "choice," enforcement, and oversight.[248] 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 Principle." 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."[249] U.S. companies must now pay greater attention to 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.[250] 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."[251] 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 U.S. 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 U.S. must obtain "the data subject's affirmative express consent."[252] 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.[253] U.S. companies must make correct use

---

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

[249] See *id.* at 6 ("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.").

[250] *Id.* at 5.

[251] GDPR, *supra* note 7, at art. 5(1)(b).

[252] EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 248, at 5.

[253] 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

of stringent EU consent mechanisms. In some instances, such as involving sensitive data, the high requirements for consent will make problematic certain kinds of data transfers.[254]

As for opt-out, the Privacy Shield makes an important change to the Safe Harbor's regime. It creates a new category within compatibility, and one 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. This language represents an EU concession to the U.S.; 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.[255] At the same time, the U.S. negotiators were able to craft a new category for opt-out, namely that of a material, but 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.

3. Enforcement and Oversight. 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."[256] The new principle concerning redress is termed, "Recourse, Enforcement and Liability Principle."[257] 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 complaint with a Privacy Shield company in the U.S.; complain to their national data protection authority; use alternative dispute resolution if the U.S.

---

health or data concerning a natural person's sex life or sexual orientation." GDPR, *supra* note 7, at art. 9(1).

[254] The health care sector in the U.S., 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 248, at 9.

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

[256] 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].

[257] EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 248, at 7.

company signs up for it; and make use of the "Privacy Shield Panel," an arbitration mechanism that permits binding decisions against U.S. companies.[258]

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.[259] 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.[260] The aim is to document factual changes compared to the record that had been before the *Schrems* Court in 2015. The step is a prudent one, taken in anticipation of future litigation in the EU.

The fourth set of core principles regards oversight.[261] 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.[262] There is also an annual joint review of the Privacy Shield by EU and U.S. officials.[263] While the Safe Harbor included a limited number of these concepts, the Privacy Shield adds to the oversight list and heightens the overall requirements. 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 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."[264] 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."[265]

---

[258] Transatlantic Data Flows, *supra* note 256. For the redress mechanisms regarding U.S. intelligence, see *id.*

[259] *Id.*

[260] *Id.*

[261] The oversight principles are primarily anchored in the "Recourse, Enforcement, and Liability" principle. EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES, *supra* note 248, at 7.

[262] *Id.* at 25-26.

[263] *Id.* at 31.

[264] *Remarks*, *supra* note 243.

[265] *Id.*

D. 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 alike 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 U.S. had occurred "within a common technological context."[266] 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."[267]

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 U.S. 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 a playing a key role in twenty-first century international relations.[268]

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 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."[269]

As in the 1990's, the platforms for computing are largely American in origin. The EU and U.S. 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 1980's, Thomas Hughes argued that those who lived in the industrial world inhabited a common "made environment" shaped by the technological systems of that day.[270] 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.[271]

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

---

[266] COLIN J. BENNETT, REGULATING PRIVACY 150 (1992).
[267] *Id.* at 6.
[268] ANNE MARIE SLAUGHTER, A NEW WORLD ORDER 20 (2004).
[269] BENNETT, *supra* note 266, at 247.
[270] HUGHES, *supra* note 229, at 184.
[271] 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.

companies have pivoted from a role as silent helpers of U.S. intelligence agencies to defenders of privacy. 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."[272] European customers have not hesitated to make these corporations realize the full extent of their dependency "on free flow of information of information across borders."[273] One estimate is of "lost profits in the billions of dollars" in the EU for these companies.[274]

As they lost sales, these organizations distanced themselves from the American national security apparatus. The *Microsoft Ireland* litigation marks a turning point in this regard.[275] 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.[276] Other leading U.S. technology companies are similarly resisting law enforcement demands for information.[277]

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.[278] In her view, European industry should be able to do more with personal information than data protection currently permits.[279] 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," which it views as dependent on access to the personal data of drivers.[280]

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

---

[272] Farrell & Newman, *supra* note 4.

[273] *Id.*

[274] Ned Schultheis, *Warrants in the Clouds*, 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.

[275] 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).

[276] 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).

[277] 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).

[278] *Merkel Calls for Balanced Approach to Data Protection*, THE REGISTER (Nov. 22, 2016), http://www.theregister.co.uk/2016/11/22/merkel_data_protection_big_data/.

[279] *Id.*

[280] 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). On activities of German auto-makers involving connected cars, see William Boston, *Intel Buys Into Auto Technology*, WALL ST. J. (Jan. 3, 2017).

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."[281] 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 "digital a driver for growth."[282]

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.[283] In our view, however, the EU and U.S. 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 U.S. 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 U.S.[284] 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 N.S.A.[285] 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.[286] As for the judiciary, the European Court of Justice generally concedes that issues of national security and criminal justice fall outside the scope of EU law.[287] 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.[288]

Finally, the EU and U.S. have deeply shared concerns regarding international terrorism and organized criminality.[289] There are also signs of increased trans-atlantic cooperation around these issues, including the signing of a new EU-U.S. "Umbrella

---

[281] Transatlantic Data Flows, *supra* note 256.

[282] *Id.*

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

[284] 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).

[285] *See* David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide*, 14 INT. J. CONSTITUTIONAL 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.").

[286] Winston Maxwell, *Systematic Government Access to Private-Sector Data in France*, 4 INT'L DATA PRIVACY LAW 4 (2014)

[287] Cole & Fabbrini, *supra* note 285, at 222.

[288] *Id.* at 225.

[289] *Id.* at 223.

Agreement" in June 2016 to permit sharing of data "to combat crime, including terrorism."[290] In sum, there are ample indications that a new post-Snowden status quo around national security surveillance will be reached.

2. Divergence. While pressure exists in the EU and U.S. 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 U.S.[291] Today, there are still omnibus laws in the EU and a patchwork of sectoral ones in the U.S. 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.[292] No similar constitutional interests exist in the U.S., and there is no similar dynamic for 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 U.S. 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 system also guarantees assistance from an independent national data privacy commissioner. In contrast, the U.S. 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."[293]

A final 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.[294] In the U.S., in *Spokeo*, the Supreme Court opened the door for a constitutionalization of "privacy harms."[295] 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 *Locherner-ization* of legislative power.[296] For the *Lochner* Court, a state law limiting the working

---

[290] *Signing of the Umbrella Agreement: A major step forward in E.U.-US relations*, EUROPEAN COMMISSION (June 2, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm.
[291] BENNETT, *supra* note 266, at 152–54.
[292] FABBRINI, *supra* note 28, at 13–14.
[293] HOOFNAGLE, *supra* note 83, at 345.
[294] GDPR, *supra* note 7, at art. 82(1).
[295] Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1550 (2016).
[296] Lochner v. New York, 198 U.S. 45 (1905).

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.[297] As in *Lochner v. New York*, however, the Supreme Court again appears ready to identify requirements in the Constitution, namely in its Article III, that will limit the ability of legislatures to protect individuals.[298]

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 U.S. 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 legal-ese 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 U.S.

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 "agreement about the things that are fundamental."[299] 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 U.S. start with profoundly different perspectives on the individual as bearer of privacy interests. But a new set of doctrines and institutions in the EU and U.S. are now tasked with developing this area of law. These institutions represent a new way for the EU and U.S. 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.[300]

In our view, the future for data privacy will not be driven by a "Brussels Effect" based on de facto unilateralism.[301] 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.[302] Rather than a "Brussels Effect," international data privacy law now features the kinds of "harmonizing networks" that Ann 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.[303] Slaughter observes, "The more that

---

[297] 300 U.S. 379, 392–93 (1937).

[298] 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).

[299] BENJAMIN N. CARDOZO, THE GROWTH OF THE LAW 144 (1924).

[300] CONSUMER DATA PRIVACY, *supra* note 12, at 31.

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

[302] *Id.*

[303] SLAUGHTER, *supra* note 268, at 5.

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."[304]

The GDPR and Privacy Shield create the most important of the new institutions and processes for potentially facilitating "interoperable privacy regimes." The future of transatlantic data trade will turn on concessions and compromises within this framework, which is more diffuse and offers more points of contact than previously. This Article now taked inventory of this structure and identifies the most critical open issues.

The GDPR assigns new powers to a European Data Protection Board and details the many tasks for it and national data protection commissions. Along with the judiciary, these institutions will play an important role in resolving key doctrinal questions. For example, today's digital economy is largely based on different premises, for better or worse, than that reflected in a wide range of requirements found in the GDPR. These include "necessity" for data processing; compatibility of data use; "purpose limitation"; and the ban on "tying." Today, a consumer frequently trades her personal data, whether or not she is aware of this exchange, for some kind of service or benefit. In turn, a company generates value by offering personalized ads, selling data to third parties, or finding other ways to turn a profit from consumer information.[305]

In an acknowledgment of these practices, the EU is developing a directive for digital content that acknowledges the validity of exchanges "against counterperformance other than money."[306] This draft Directive permits a data subject to create contracts for digital content and services by supplying her personal information.[307] It also avoids answering certain hard questions about privacy. Rather, it contains a "savings clause" to the effect that the Digital Content Directive is "[w]ithout prejudice to the rules on data protection" found in EU law.[308] In years to come, EU law will be obliged to assess the legitimacy of business models based around data trade. Dammann has perceptively observed that the "cardinal question" in this regard will be the "level of abstraction at which a business goal ... is to be decided."[309] In doing so, a key concern will be the interpretation of "compatibility" as expressed in the GDPR's "purpose limitation."[310] As the language of Article 5(1)(b) of the GDPR makes clear, a compatible purpose is one that is "specified, explicit, and legitimate."[311] The question of "legitimacy" will be central to decision-making about the permissibility of digital services, digital contracts, and data protection in the EU.

---

[304] *Id.* at 162.
[305] For further discussion, see Schwartz, *supra* note 100.
[306] Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 16 Com (2015) 634 final (Dec. 9, 2015).
[307] *Id.* at 11.
[308] *Id.* at 20.
[309] Dammann, *supra* note 155, at 312.
[310] GDPR, *supra* note 7, art. 6.
[311] *Id.* at art. 5(1)(b).

The GDPR also structures interactions with non-EU countries around issues relating to international data transfers. The GDPR assigns important power to the Commission to "enter into consultations" with third countries that may no longer ensure an adequate level of protection. Further, 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 of legislation for the protection of personal data."[312] These parts of the GDPR demonstrate the EU's commitment to shaping data privacy law through international dialogue.

As for the Privacy Shield, its institutional arrangements represent the kind of a "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 act to resolve complaints by these parties; and an independent Ombudsperson is to interact with U.S. national security agencies.[313] There is also a process for the Commission and Department of Commerce to collaborate on an annual joint review.[314]

As a further example of this joint "lawmaking," one can point to future decisions about novel doctrinal concepts, such as that of a "material change" in the grounds for processing that is still "compatible." Resolution of this issue will, in turn, be important for development of EU data protection. The result is that officials and individuals in the EU and U.S. are now part of a disaggregated network tasked with devising new solutions for harmonizing their underlying views of data privacy.

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.[315] 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.

There can be some hope, therefore, that the European Court of Justice in its future assessments will operate in a fashion similar to Europe's national constitutional courts. In the analysis of Stone Sweet, these courts frequently enable

---

[312] *Id.* at art. 50(a).
[313] Transatlantic Data Flows, *supra* note 256.
[314] *Id.*
[315] *Schrems, supra* note 9, at ¶ 21.

corrective processes that bring other governmental bodies into dialogue with it.[316] They often favor judgments that permit "corrective revision efforts" and only "partial victories."[317] 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.

V. 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*."[318]

In placing limits on certain possible choices, EU data protection has acted to restrict the collective negative impact of individual trade in personal information.[319] 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 restrictions on contract and consent. In contrast, the U.S. lacks any similar constitutionalization of its information privacy law and proceeds through a sectoral legislative approach. The U.S. is interested in 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 be in accord with those goals. At a high level, the EU and U.S. recognize the value of both data privacy and the free flow of information. 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 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

---

[316] SWEET, *supra* note 27, at 82.

[317] *Id.* at 142.

[318] EGGERS, *supra* note 228, at 261.

[319] A number of 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 take into account "the social impacts of individual privacy decisions." Solove, *supra* note 212, 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.

between the EU and U.S. with numerous opportunities for harmonization, coordination, and cooperation. These legal documents offer a fresh start for the EU and U.S. in resolving conflicts about data privacy.