THE EU-U.S. PRIVACY COLLISION: A TURN TO INSTITUTIONS AND PROCEDURES

Paul M. Schwartz[*]

I. INTRODUCTION

Internet scholarship in the United States generally concentrates on how decisions made in this country about copyright law, network neutrality, and other policy areas shape cyberspace.[1] In one important aspect of the evolving Internet, however, a comparative focus is indispensable. Legal forces outside the United States have significantly shaped the governance of information privacy, a highly important aspect of cyberspace, and one involving central issues of civil liberties. The EU has played a major role in international decisions involving information privacy, a role that has been bolstered by the authority of EU member states to block data transfers to third party nations, including the United States.[2]

The European Commission's release in late January 2012 of its proposed "General Data Protection Regulation" (the Proposed Regulation) provides a perfect juncture to assess the ongoing EU-U.S. privacy collision.[3] An intense debate is now occurring about critical areas of information policy, including the rules for lawfulness of personal processing, the "right to be forgotten," and the conditions for data flows between the EU and the United States.

This Article begins by tracing the rise of the current EU-U.S. privacy status quo. The European Commission's 1995 Data Protection Directive (the Directive) staked out a number of bold positions, including a limit on international data transfers to countries that lacked "adequate" legal protections for personal information.[4] The impact of the

[*] Professor of Law, University of California, Berkeley, School of Law; Director, Berkeley Center for Law & Technology. For their insightful comments on earlier drafts, I wish to thank Jesse Koehler, Ronald Lee, Katerina Linos, Anne Joseph O'Connell, Karl-Nikolaus Peifer, Joel Reidenberg, Spiros Simitis, Daniel Solove, Latanya Sweeney, and Daniel Weitzner. All translations are my own.

[1] *See generally, e.g.*, TIM WU, THE MASTER SWITCH (2010); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET — AND HOW TO STOP IT (2008).

[2] *See infra* section II.B, pp. 1971–79.

[3] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed Regulation*].

[4] *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the

Directive has been considerable. The Directive has shaped the form of numerous laws, inside and outside of the EU, and contributed to the creation of a substantive EU model of data protection, which has also been highly influential.[5]

This Article explores the path that the United States has taken in its information privacy law and explores the reasons for the relative lack of American influence on worldwide information privacy regulatory models. As an initial matter, the EU is skeptical regarding the level of protection that U.S. law actually provides. Moreover, despite the important role of the United States in early global information privacy debates, the rest of the world has followed the EU model and enacted EU-style "data protection" laws.

At the same time, the aftermath of the Directive has seen ad hoc policy efforts between the United States and EU that have created numerous paths to satisfy the EU's requirement of "adequacy" for data transfers from the EU to the United States.[6] The policy instruments involved are the Safe Harbor, the two sets of Model Contractual Clauses, and the Binding Corporate Rules.[7] These policy instruments provide key elements for an intense process of nonlegislative lawmaking, and one that has involved a large cast of characters, both governmental and nongovernmental.

This Article argues that this policymaking has not been led exclusively by the EU, but has been a collaborative effort marked by accommodation and compromise. In discussing this process of nonlegislative lawmaking, this Article will distinguish the current policymaking with respect to privacy from Professor Anu Bradford's "Brussels Effect."[8] This nonlegislative "lawmaking" is a productive outcome in line with the concept of "harmonization networks" that Professor Anne-Marie Slaughter has identified in her scholarship.[9] "Harmonization networks" develop when regulators in different countries work together to harmonize or otherwise adjust different kinds of domestic law to achieve outcomes favorable to all parties.[10]

The Article then analyzes the likely impact of the Proposed Regulation, which is slated to replace the Directive. The Proposed Regulation threatens to destabilize the current privacy policy equilibrium and prevent the kind of decentralized global policymaking that has oc-

---

Free Movement of Such Data, art. 25, 1995 O.J. (L 281) 31, 45–46 [hereinafter Data Protection Directive].

5 *See infra* section II.B.2, pp. 1973–79.

6 Data Protection Directive, *supra* note 4, art. 25(2), at 45.

7 *See infra* section II.C, pp. 1979–92.

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

9 *See generally* ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER 59–61 (2004).

10 *Id.* at 59.

curred in the past. The Proposed Regulation overturns the current balance by heightening certain individual rights beyond levels that U.S. information privacy law recognizes.[11] It also centralizes power in the European Commission in a way that destabilizes the policy equilibrium within the EU, and thereby threatens the current policy processes around harmonization networks.[12]

To avert the privacy collision ahead, this Article advocates modifications to the kinds of institutions and procedures that the Proposed Regulation would create.[13] A "Revised Data Protection Regulation" should concentrate on imposing uniformity only on "field definitions," that is, the critical terms that mark the scope of this regulatory field. The Revised Regulation should be clear that member states can supplement areas that do not fall within its scope with national measures. This approach would leave room for further experiments in data protection by the member states. The Revised Regulation should also alter the currently proposed procedures to limit the Commission's assertion of power as the final arbiter of information privacy law.

II. THE RISE OF THE EU-U.S. STATUS QUO

The EU has played a major role in the global privacy debate since the 1990s. Its Data Protection Directive[14] and, more recently, its proposed General Data Protection Regulation[15] have sought to establish de facto international benchmarks for corporate information processing. As the *Wall Street Journal* noted in 2003, EU privacy rules "are increasingly shaping the way businesses operate around the globe."[16]

In this Part, I first trace the early history of EU-U.S. information privacy law. I then describe and analyze the elements of the EU-U.S. status quo that emerged in the wake of the Directive. The Directive developed elements of an EU model of information privacy law that has proven internationally influential and that differs from the U.S. approach in important ways. Nonetheless, significant international "lawmaking" has taken place subsequent to the Directive, and the resulting policy instruments provide multiple ways to harmonize the EU and U.S. models.

---

[11] *See infra* section III.A.1, pp. 1994–97.

[12] *See infra* section III.A.2, pp. 1997–2001.

[13] *See infra* section III.C, pp. 2003–08.

[14] Data Protection Directive, *supra* note 4.

[15] *Proposed Regulation*, *supra* note 3.

[16] David Scheer, *For Your Eyes Only — Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL ST. J., Oct. 10, 2003, at A1.

A. The Early History of EU Data Protection Law

The history of European data protection law does not start with the Directive. Rather, it begins within an individual country, and with a state-level law: the Hessian Parliament enacted the world's first comprehensive information privacy statute in Wiesbaden, Germany, on September 30, 1970.[17] This law was followed by those of other German states,[18] and in 1977 by a federal German law.[19] Other EU nations enacted data protection statutes as well: among the first wave of legislation were statutes in Sweden (1973), Austria (1978), Denmark (1978), France (1978), and Norway (1978).[20]

By the end of this period, there was a consensus that information privacy statutes were to be constructed around Fair Information Practices (FIPs). This approach, shared in the United States and Western Europe alike, defines core obligations for organizations, whether in the public or private sector, that process personal information.[21] The U.S. government and American privacy experts played an important part in this early global privacy debate. For example, a white paper from an advisory committee to the Secretary for Health, Education, and Welfare in the United States contained an influential early formulation of FIPs.[22]

There were also important supranational privacy agreements that preceded the EU Data Protection Directive of 1995. The two most important are the Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) and the Convention on Privacy of the Council of Europe.[23] The OECD is a group of leading

---

[17] Spiros Simitis, *Einleitung: Geschichte — Ziele — Prinzipien [Introduction: History — Goals — Principles]*, *in* KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [COMMENTARY ON THE FEDERAL DATA PROTECTION LAW] 76, 77 (Spiros Simitis ed., 7th ed. 2011).

[18] *Id.* at 77–78.

[19] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung [Bundesdatenschutzgesetz] [BDSG] [Law to Protect Against Misuse of Personal Data in Data Processing [Federal Data Protection Law]], Jan. 27, 1977, BUNDESGESETZBLATT, Teil I [BGBL. I] at 201, repromulgated Jan. 14, 2003, BGBL. I at 66, last amended by Gesetz zur Änderung datenschutzrechtlicher Vorschriften [Law Amending Data Protection Provisions], Aug. 14, 2009, BGBL. I at 2814.

[20] *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY 127 (2006); Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY 219, 221, 226 (Philip E. Agre & Marc Rotenberg eds., 1997).

[21] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 915–17 (4th ed. 2011).

[22] *See generally* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

[23] Org. for Econ. Co-operation & Dev. [OECD], *Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C(80)(58) final (Oct. 1, 1980) [hereinafter OECD Guidelines], *reprinted in* 20 I.L.M. 422, *available at* http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtrans

industrial countries, including the United States, concerned with economic and democratic development. Its Privacy Guidelines were the first international statement of essential information privacy principles. Although the OECD principles are nonbinding, the Guidelines have influenced national legislation.[24]

The Council of Europe is an intergovernmental organization, established in 1949, that promotes unity among European nations.[25] Throughout the 1980s, the Council's Data Protection Convention was the most important Europe-wide agreement regarding the processing of personal information.[26] Like the subsequently established Directive, the Convention seeks to provide a central point of reference for national regulations.[27]

Persistent themes throughout the history of EU-U.S. privacy law were already manifest in this early period. First, there has long been a significant EU-U.S. policymaking interplay, which in this period included discussions of the policy instruments of FIPs and the development of the nonbinding OECD Guidelines.[28] Indeed, the international debate has been influenced by the legal roots of privacy in the United States, including the famous essay on privacy by Samuel Warren and Louis Brandeis from 1890.[29] The German Federal Constitutional Court and the German Federal Court of Justice have referenced "*das Recht, allein gelassen zu werden*" (the right to be let alone) and, in some cases, cited to Warren and Brandeis.[30] In 2012, a law review in Germany even published a complete German translation of Warren and Brandeis's essay over one hundred and twenty years after its first

---

borderflowsofpersonaldata.htm; Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108 [hereinafter Convention on Privacy], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[24] Simitis, *supra* note 17, at 151–54.

[25] COLIN J. BENNETT, REGULATING PRIVACY 133–36 (1992).

[26] This European treaty was opened for signature in 1981; it is a non-self-executing treaty, which means that it requires signatory nations to establish domestic data protection statutes that give effect to its principles and provide a common core of safeguards. *Id.* at 135–36.

[27] Simitis, *supra* note 17, at 138–51.

[28] *See* BENNETT, *supra* note 25, at 138 (noting how the OECD and its Guidelines "provided a unique opportunity for both Americans and Europeans to debate the safeguarding of human rights in the computer age"). Professor Colin Bennett also finds a process of incorporation of FIPs that over time was built around a "policy community" and "international organizations." *Id.* at 222.

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

[30] Bundesgerichtshof [BGH] [Federal Court of Justice] Dec. 19, 1995, 131 ENTSCHEIDUNGEN DES BUNDESGERICHTSHOFES IN ZIVILSACHEN [BGHZ] 332, 337 (citing Warren & Brandeis, *supra* note 29, at 193); Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] June 5, 1973, 35 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] 202, 233 (recognizing a right "*allein gelassen zu werden*," that is, "a right to be let alone"); *see also Dokumentarfilm über Soldatenmord von Lebach* [*Documentary About the Murder of Soldiers in Lebach*], 2000 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 1859.

publication.[31] In an introduction to the publication, Thilo Weichert, the data protection commissioner of the German state of Schleswig-Holstein, noted the "amazing timeliness" of the essay for current discussions of information privacy.[32] The European Court of Human Rights has also cited to this important concept from American law.[33]

Second, the international debate about information privacy has never been confined to human rights *or* data trade. It has always been about both. The OECD Guidelines and the Council's Convention both pay careful attention to individual privacy rights. The OECD's rationale for the Guidelines mentions the dangers of "violations of fundamental human rights" through the processing of personal data.[34] At the same time, it also talks about the "danger that disparities in national legislations could hamper the free flow of personal data across frontiers."[35] At a 2010 roundtable in Paris on the thirtieth anniversary of the OECD Guidelines, Michael Kirby, the Chairman of the OECD's expert group on privacy from 1978 to 1980, noted that the initial impetus for the OECD's work was "to contribute to (and defend) free flows deemed suitable to market information economies."[36] Finally, the Council's Convention on Privacy speaks in its Preamble of the goal of "reconcil[ing] the fundamental values of the respect for privacy and the free flow of information between peoples."[37]

B. The Data Protection Directive

We now move from the early history of EU information privacy law to the Data Protection Directive. A popular tool of EU lawmaking, directives are generally not immediately binding but are "harmonizing" instruments; they require member states to enact national legis-

---

[31] Samuel D. Warren & Louis D. Brandeis, *Das Recht auf Privatheit — The Right to Privacy* (Marit Hansen & Thilo Weichert trans.), 36 DATENSCHUTZ UND DATENSICHERHEIT 755 (2012).

[32] Thilo Weichert, *Anmerkungen zu Warren/Brandeis — Das Recht auf Privatheit* [*Comments on Warren/Brandeis — The Right to Privacy*], 36 DATENSCHUTZ UND DATENSICHERHEIT 753, 753 (2012).

[33] Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 41, 78 (Zupančič, J., concurring) (noting that "[p]rivacy . . . is the right to be left alone").

[34] *Internet Economy — OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Mar. 30, 2013).

[35] *Id.*

[36] Michael Kirby, Former Chair of the OECD Expert Group on Transborder Data Barriers and Privacy Protection, Speech at the Round Table on the 30th Anniversary of the OECD Guidelines on Privacy (Mar. 10, 2010), *available at* http://www.oecd.org/internet/interneteconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm. The expert group on privacy that Kirby headed was responsible for writing the OECD Guidelines.

[37] Convention on Privacy, *supra* note 23, pmbl.

lation that reflect their principles.[38] The Data Protection Directive established common rules for information privacy among EU member states and set these states a three-year deadline to enact conforming legislation.[39] The Directive built on existing national legislation and modeled many of its aspects on such statutes, which meant that some member states merely had to enact amendments to existing law. As Professor Spiros Simitis, a leading international data protection law expert, observes, the Commission "sought to combine the guiding principles of national data protection laws" in the Directive.[40] The result, according to Simitis, was not a "simple reproduction,"[41] but a "patchwork" in the Directive that reflects corrections and modifications of these national elements as well as various compromises.[42]

1. Elements of the Data Protection Directive. — The chief goals of the Directive are: (1) to facilitate the free flow of personal data within the EU, and (2) to ensure an equally high level of protection within all countries in the EU for "the fundamental rights and freedoms of natural persons, and in particular their right to privacy."[43] Within the EU, the 1990s were a period of increased economic activity and of heightened demands for personal information. In the absence of EU-wide standards, data transfers within the EU had the potential to undermine the efforts, dating back to the 1970s, of individual member states to protect the personal information of their citizens.[44]

The resulting regulatory approach combined economic liberalization of trade involving personal data with harmonized policies to protect civil liberties.[45] The Directive's protection also extends outside of the EU; the Directive contains important provisions concerning international data transfers.[46] This extraterritorial approach is a common feature of EU regulation.[47] The Commission's concern for certain policy matters, such as antitrust or the environment, can require attention

---

[38] *See* GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW 430 (1993).

[39] Data Protection Directive, *supra* note 4, art. 32(1), at 49–50.

[40] Simitis, *supra* note 17, at 166.

[41] *Id.*

[42] *Id.* at 167 (quoting COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [NATIONAL COMMISSION ON INFORMATION TECHNOLOGY AND LIBERTIES], 11E RAPPORT D'ACTIVITÉ 1990 [11TH ACTIVITY REPORT 1990] 33 (1991)).

[43] Data Protection Directive, *supra* note 4, art. 1, at 38.

[44] *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 480–81 (1995).

[45] On this tension between these interests in the background of the EU Data Protection Directive, see Spiros Simitis, *Einleitung*, *in* EG-DATENSCHUTZRICHTLINIE [EU DATA PROTECTION DIRECTIVE] 61, 61–63 (Ulrich Dammann & Spiros Simitis eds., 1997).

[46] Data Protection Directive, *supra* note 4, arts. 25–26, at 45–46.

[47] Bradford, *supra* note 8, at 38–39.

to the activities of non-EU nations or entities located outside the EU.[48] Globalization of world data flows called for EU action with just such an international reach. Simitis summarizes this aspect of EU law: "Data protection does not stop at national borders. Transfers of information must be bound to conditions that attempt in a targeted fashion to protect the affected parties."[49]

Article 25 of the Directive permits transfers to "third" countries, that is, countries outside of the EU, only if these nations have "an adequate level of protection."[50] This restriction on transfers to third countries reflects an underlying belief that personal information of EU citizens merits protection throughout the world and not merely within the EU. Prior to the Directive, some data protection laws in member states had placed similar restrictions on transfers to third countries that provided an insufficient level of legal privacy protection.[51]

Under the Directive, a decision as to adequacy is generally made at the member state level, although the European Commission may "enter into negotiations" with countries with inadequate data protection "with a view to remedying the situation."[52] The Directive also provides limited exceptions to its adequacy standard and details the approach for determining the level of protection provided by countries outside the EU. It calls for an evaluation of adequacy "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations."[53] Hence, it requires a contextual analysis of the protections in place in the non-EU country. Article 25 of the Directive further specifies that "particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, . . . the rules of law . . . in force in the third country in question and the professional rules and security measures . . . in that country."[54]

2. The Impact of the Directive: The Form and Substance of an EU Model. — The impact of the Directive has been significant. First, it has shaped the form of numerous laws, inside and outside the EU. Second, it has contributed to the development of a substantive EU model of data protection, which has been highly influential. Regarding each of these two elements, the United States has proved to be an outlier.

With respect to shaping the form of data protection law, the Directive has encouraged the rise of omnibus legislation throughout the

---

48 *See id.* at 21–22.
49 Simitis, *supra* note 17, at 125.
50 Data Protection Directive, *supra* note 4, art. 25(1), at 45.
51 Schwartz, *supra* note 44, at 488–92.
52 Data Protection Directive, *supra* note 4, art. 25(5), at 46.
53 *Id.* art. 25(2), at 45.
54 *Id.* at 45–46.

EU and most of the world. "Omnibus" privacy laws establish regulatory standards with a broad scope.[55] Under the omnibus approach, sectoral laws are a backup used to increase the specificity of regulatory norms stemming from the initial statutory framework. As Professor David Flaherty already observed in 1989, sectoral laws respond to "a particular type of problem" and "grant specific enforceable rights to individuals."[56] By requiring EU member states to transpose its requirements into national law, the Directive created strong incentives for omnibus legislation within the EU. Enactment of such legislation requires attention to only a relatively limited set of benchmarks — ones that a single statute can express.[57] An omnibus law also provides a relatively clear target for the assessment of "adequacy."[58] Finally, privacy pioneers among EU member states had already anchored their information privacy statutes in omnibus legislation, which encouraged other countries to follow this path.[59]

The Directive's requirements have followed the EU in its eastward expansion. From fifteen member states in 1995, the EU has now expanded to twenty-seven as of 2013.[60] The new members of the EU have all enacted omnibus laws.[61] As discussed below, the omnibus privacy model has also greatly influenced the shape of legislation outside of the EU.[62]

The United States has been the great exception regarding the international preference for omnibus legislation. It regulates information privacy on a sector-by-sector basis. The United States also has different statutes for the public and private sectors. Within the private sector, it concentrates on the data holder and, in some instances, on the type of data. As an example, the applicable laws do not provide medical information as a category with a uniform level of protection. If personal information is held by a "covered entity" under the Health Information Portability and Accountability Act of 1996[63] (HIPAA), it is protected by one set of rules.[64] If a school regulated by the Family

---

55 SOLOVE & SCHWARTZ, *supra* note 21, at 1110.

56 David H. Flaherty, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 404–05 (1989).

57 Paul M. Schwartz, Feature, *Preemption and Privacy*, 118 YALE L.J. 902, 915 (2009).

58 *Id.* at 923.

59 *Id.* at 914–16.

60 *Countries*, EUR. UNION, http://europa.eu/about-eu/countries/index_en.htm (last visited Mar. 30, 2013).

61 The best single source for these statutes is *Privacy Library*, MORRISON & FOERSTER LLP, http://www.mofo.com/privacylibrary/PrivacyLibraryLanding.aspx?xpST=PrivacyLibraryLanding (last visited Mar. 30, 2013).

62 *See infra* p. 1979.

63 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

64 *See generally* Health Insurance Portability and Accountability Act Regulations, 45 C.F.R. pt. 164 (2012).

Educational Rights and Privacy Act of 1974[65] (FERPA) holds medical information, it may be subject to a different set of rules or, perhaps, additional rules.[66] If the information does not fall into either category and is not covered by any of the other various substantive information privacy regimes, then it might not be protected at all.

In some U.S. privacy statutes, a further distinction relates to the form in which the data is held, or the content of the information. FERPA regulates only information that is found in "educational records";[67] the Video Privacy Protection Act of 1988[68] covers only "prerecorded video cassette tapes or similar audio visual materials";[69] and the Fair Credit Reporting Act[70] reaches only credit reports.[71] By contrast, under the EU's omnibus approach, the law protects data regardless of the entity that holds it, or the type of information in a record. Further regulatory distinctions are drawn when a sectoral law is in place, but even here, omnibus laws fill in gaps in the sectoral statute.[72]

Shifting from form to substance, there are substantive similarities and dissimilarities between the EU and U.S. models of information privacy. As I noted in section II.A, these legal systems share an approach centered around FIPs for personal information. Due to the shared focus on these regulatory norms, some observers in the 1990s argued that a convergence of global regulatory approaches had occurred. For example, Professor Colin Bennett concluded: "The process of policy making in the data protection area is clearly one where broad transnational forces for convergence have transcended variations in national characteristics."[73] No single privacy statute contains all the FIPs in the same fashion or form, but Bennett's idea was that international agreement had been reached on privacy regulation's fundamental elements.[74]

---

[65] 20 U.S.C. § 1232g (2006 & Supp. V 2011).

[66] One critical factor will be whether the educational institution is also a "covered entity" under HIPAA. *See* 45 C.F.R. § 160.103. For a discussion of the types of health care plans and health care providers that fall into this category, see WILLIAM H. ROACH, JR., ET AL., MEDICAL RECORDS AND THE LAW 141–45 (4th ed. 2006). Another factor will be whether the data is stored in a form that constitutes an "education record" under FERPA. *See, e.g.*, 20 U.S.C. § 1232g(b)(2). For a discussion of this second factor, see Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1823 (2011).

[67] 20 U.S.C. § 1232g.

[68] 18 U.S.C. § 2710 (2006), *amended by* Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013).

[69] 18 U.S.C. § 2710(a)(4).

[70] 15 U.S.C. §§ 1681–1681x (2006 & Supp. V 2011).

[71] *See, e.g.*, *id.* §§ 1681a–1681b.

[72] The German Federal Data Protection Law makes explicit the relationship between the different regulatory levels. *See* BDSG, *supra* note 19, Jan. 14, 2003, BGBL. I at 66, art. 1, § 1(3).

[73] BENNETT, *supra* note 25, at 150.

[74] *See id.* at 152.

Bennett was correct that some agreement exists worldwide regarding the basic regulatory principles of information privacy. This degree of consensus exists despite the fact that Europe has opted for omnibus privacy statutes, while the United States prefers sectoral ones. Yet the dissimilarities resulting from this policy divide are significant. Some are a matter of degree, and some are a matter of kind. In the former category are certain interests that exist in both legal systems, but are more heavily emphasized in EU law. In particular, the EU places greater emphasis on the following FIPs: (1) limits on data collection, also termed data minimization; (2) the data quality principle; and (3) notice, access, and correction rights for the individual. In the United States, by contrast, there has been only a limited reliance on a stripped-down concept of notice of data processing practices. A strong reliance on the affected party's consent to data processing accompanies the emphasis on notice in the United States; the EU's FIPs discuss consent but place much less weight on it.[75]

Some FIPs are found exclusively in the EU regime. These EU elements are: (4) a processing of personal data made only pursuant to a legal basis; (5) regulatory oversight by an independent data protection authority; (6) enforcement mechanisms, including restrictions on data exports to countries that lack sufficient privacy protection; (7) limits on automated decisionmaking; and (8) additional protection for sensitive data.[76] As an initial example of such a distinction between the two legal systems, the United States does not rely on a notion that personal information cannot be processed in the absence of a legal authorization. Rather, it permits information collection and processing unless a law specifically forbids the activity. U.S. law accepts "regulatory parsimony": before the U.S. legal system acts, the lawmaker will wait for strong evidence that demonstrates the need for a regulatory measure.[77]

The First Amendment's protections for freedom of expression also help define the U.S. orientation to privacy regulation. The First Amendment can *bolster* privacy — one way that it does so is through its protection of freedom of association.[78] More to the point, however, the First Amendment can also *restrict* information privacy: statutes

---

[75] For a critique of using a market-based consent model, such as the one seen in the United States, see Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1681–87 (1999).

[76] For a description of the EU model of FIPs, see generally CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW 63–108 (2d ed. 2007).

[77] *See* Schwartz, *supra* note 57, at 913–14 (contrasting an EU approach to information privacy based on the prevention of harm with a U.S. orientation that is based, in part, on "regulatory parsimony" and, in particular, on avoiding any unnecessary regulation of information flows).

[78] *See, e.g.*, NAACP v. Alabama, 357 U.S. 449, 462–66 (1958) (holding that the First Amendment protects group membership lists against state disclosure laws to protect individual members against "exposure of their beliefs shown through their associations," *id.* at 463).

that limit information sharing on privacy grounds are subject to constitutional scrutiny of their impact on the speech of the data processor. In *Sorrell v. IMS Health Inc.*,[79] for example, the Supreme Court reaffirmed this commitment to the First Amendment as a force that prevents certain privacy protective measures. It struck down a Vermont law that prohibited the sale, disclosure, and use of pharmacy records by "detailers," who used the information to help target doctors for the sale of prescription pharmaceuticals.[80] The Supreme Court stated that "[s]peech in aid of pharmaceutical marketing . . . is a form of expression protected by the Free Speech Clause of the First Amendment."[81]

Another dramatic distinction between U.S. and EU information privacy law is that the United States does not limit data exports to other countries and has not created a national data protection commission. Despite occasional proposals in Congress to restrict the "outsourcing" of data processing to India and other countries, U.S. law currently places no limits on a company's exports of information to other countries.[82] Ironically enough, given the EU's restrictions in this area, Congress considered but failed to adopt such a limit on data exports from the United States in the 1970s when considering one of its first privacy statutes.[83]

As for oversight, the closest that the United States comes to a national data protection agency is the Federal Trade Commission (FTC). During the last two decades, the FTC has played an increased role in protecting privacy in the United States, and this development represents a highly significant change for privacy regulation on this side of the Atlantic.[84] Established in 1914, the FTC is an independent federal agency dedicated to consumer protection and the establishment of fair practices in business. By its own account, the FTC has engaged in over three hundred enforcement actions concerning privacy since 1996.[85] At the same time, there are significant limits on the scope of the FTC's activities as protector of information privacy. The FTC does not have jurisdiction over all companies, and its enforcement has not extended to even the narrow range of FIPs used in the United

---

[79] 131 S. Ct. 2653 (2011).

[80] *See id.* at 2659–60.

[81] *Id.* at 2659.

[82] SOLOVE & SCHWARTZ, *supra* note 21, at 1161–63.

[83] S. COMM. ON GOV'T OPERATIONS & SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RIGHTS OF THE H. COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUBLIC LAW 93-579), at 234 (J. Comm. Print 1976).

[84] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 284–87 (2011).

[85] Press Release, FTC, FTC Testifies Before the Senate Commerce Committee on Privacy; Industry Efforts to Implement "Do Not Track" System Already Underway (Mar. 16, 2011), *available at* http://www.ftc.gov/opa/2011/03/privacy.shtm.

States. Rather, this agency concentrates primarily on "notice and choice."[86]

Finally, U.S. law contains only limited, sector-specific protections for sensitive information.[87] It also does not generally restrict automated processing. In contrast, the Directive requires additional attention to certain types of information and additional restrictions on certain processing practices. These elements were incorporated from the French national data protection law of 1978.[88] The Directive forbids the processing of personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[89] It also contains derogations, or exceptions, from this rule.[90] As for "automated processing," the Directive articulates a suspicion of computer data processing when humans are absent from the ultimate stages of decisionmaking.[91] It requires member states to grant "the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him."[92]

At the level of form and substance then, the United States has taken a different path than the EU in regulating information privacy. The U.S. approach also gives relatively free rein to companies to try new kinds of data processing. In particular, enterprises in new business areas are largely free of regulation under a sectoral regime and thereby are able, depending on one's perspective, to test innovative new practices or find new ways to violate privacy. Another consequence of this approach is to place heavier data privacy restrictions on established enterprises in sectors regulated by privacy laws than on new companies. For example, new technology companies can make use of personal information to mine data and send tailored advertisements through the Internet in a way that statutes would prevent cable com-

---

[86] *See* FTC, PRELIMINARY FTC STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 19–21 (2010); SOLOVE & SCHWARTZ, *supra* note 21, at 820–21; Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 740–41, 743 (2001); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 887–89 (2003). For a summary of the limited triggers for FTC privacy complaints, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 135 (2013).

[87] PAUL M. SCHWARTZ & JOEL REIDENBERG, DATA PRIVACY LAW 281–82, 333–37 (1996).

[88] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978, Concerning Information Technology, Files, and Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL JOURNAL OF THE FRENCH REPUBLIC], Jan. 7, 1978, p. 227, art. 31, at 229.

[89] Data Protection Directive, *supra* note 4, art. 8(1), at 40.

[90] *See id.* art. 8(2)–(5), at 40–41.

[91] *Id.* art. 15(1), at 43.

[92] *Id.*

panies and telephone companies from doing within their respective domains.[93] The result of the sectoral approach in the United States makes newer technology companies a powerful voice in favor of the regulatory status quo.

The rest of the world has not followed the U.S. approach. In almost two decades since the enactment of the Directive, it is the EU's privacy model that has proven highly influential. According to Professor Graham Greenleaf: "[S]omething reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws."[94] He also sees the influence of these EU-style laws as having increased in recent years.[95] Other experts have pointed to the influence of EU privacy laws internationally.[96]

Nonetheless, there is a deeper process underway, and it is not the unilateral imposition of EU standards on the rest of the world. Rather, mutual accommodation around shared lawmaking has occurred. The U.S. government has successfully engaged in shaping the form and meaning of EU data protection law. U.S. companies have taken a similar path of involvement with EU regulators. Some of the highlights of this phenomenon include the development of an EU-U.S. Safe Harbor Program (2000), Model Contractual Clauses (2001, 2003), and Binding Corporate Rules (2008).[97] This Article's next section explores the results of this policy process.

C. International "Lawmaking" Under the Directive: Paths to Adequacy

Since the enactment of the 1995 Directive, there have been a number of successful negotiations involving national regulators, supranational organizations, and private entities. The key issue has concerned international transfers of data. As discussed in this Article, the Directive permits such activity only when the third party country would provide adequate protection, and the EU's consensus has been that U.S. privacy law does not, at least as a general matter, meet this re-

---

[93] *See* 47 U.S.C. § 222 (2006 & Supp. V 2011) (placing privacy restrictions on telecommunications carriers); 47 U.S.C. § 551 (2006) (placing privacy restrictions on cable companies).

[94] Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 77 (2012).

[95] *Id.*

[96] *See, e.g.*, ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY 3 (2008); Bradford, *supra* note 8, at 3.

[97] For a concise and practitioner-oriented overview of all these compliance mechanisms, see generally LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO INTERNATIONAL DATA PRIVACY LAW COMPLIANCE 25–47 (2012).

quirement.[98] The EU has never officially found that the U.S. approach to privacy is either adequate or inadequate, and the United States has never requested an adequacy determination. Nonetheless, the EU consensus is that the United States lacks an adequate level of protection. The closest to an official determination on that issue is a 1999 Opinion from the Article 29 Working Party. In the opinion, this influential group of European data protection officials states: "[T]he Working Party takes the view that the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."[99]

The Safe Harbor, Model Contractual Clauses, and Binding Corporate Rules are three policy responses that share the goal of finding a way for U.S. companies to meet the "adequacy" requirement of the Directive's Article 25. At present, however, scant attention has been paid to the underlying significance of this collaborative "lawmaking." After setting out these EU-U.S. policy encounters and exploring the policy responses, I wish to draw on two existing academic models. These are the "Brussels Effect" concept of Anu Bradford[100] and the "harmonization networks" of Anne-Marie Slaughter.[101]

1. "Lawmaking" in the Shadow of the Directive. — A period of intense international activity followed the enactment of the Directive and the harmonizing legislation of member states. The result has been a multifaceted response to the privacy agenda of the EU. It has produced the following policy instruments: an EU-U.S. Safe Harbor agreement, the Model Contractual Clauses, and Binding Corporate Rules.

(a) The Safe Harbor. — The origins of the Safe Harbor agreement date to 1998 and the start of negotiations between the U.S. Department of Commerce and the European Commission. At the start of July 2000, the Commission released the final text of the "Safe Harbor Arrangement" and a series of supporting documents.[102] That same

---

98 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussion Between the European Commission and the United States Government*, at 4, DG MARKT Doc. 5092/98, WP 15 (Jan. 26, 1999).

99 *Id.* at 2.

100 Bradford, *supra* note 8.

101 SLAUGHTER, *supra* note 9, at 59–61.

102 The EU-U.S. Safe Harbor Arrangement was laid out in final documents issued in the United States in July and September 2000 and in the EU in July 2000. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000); Issuance of Safe Harbor Principles and Transmission to European Commission; Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 (Sept. 19, 2000); Commission Decision 2000/520/EC of 26 July 2000, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles

month, the EU Parliament rejected the agreement in a nonbinding resolution before the Commission approved it on July 25, 2000.[103]

The resulting framework creates a voluntary self-certification program for U.S. firms. It is a negotiated mixture of EU-U.S. standards, and one that ends somewhat closer to the EU version rather than the U.S. version of privacy norms.[104] Compliance with these standards is overseen by U.S. federal agencies, most notably the FTC.[105] Pursuant to the Safe Harbor Agreement, the FTC has found violations of this international agreement in 2011 and 2012 by Google[106] and Facebook,[107] respectively. On the positive side for U.S. companies, most claims brought by European citizens against U.S. companies will be brought in the United States and pursuant to U.S. legal principles.[108] Finally, and most significantly, companies participating in the Safe Harbor are deemed to provide adequate protections, and EU data flows to them can continue.[109] A member state does not need to make a prior approval of a data transfer to the United States.

(b) Model Contractual Clauses. — As another part of the response to the adequacy requirement, the EU has approved two sets of Model Contractual Clauses. The Directive provides a framework for this process in Article 26(2), which permits transfers to companies in third countries where there are "appropriate contractual clauses."[110] A contract is a way to tailor a response to the issue of adequacy; the party transferring the personal information and the one receiving it can pledge to provide protections that will be adequate.

---

and Related Frequently Asked Questions issued by the US Department of Commerce, 2000 O.J. (L 215) 7 [hereinafter Commission Safe Harbour Decision].

103 For the rejection of the agreement by the European Parliament, see Resolution on Report A5-0177/2000 of the European Parliament on the Safe Harbour Privacy Principles, 2001 O.J. (C 121) 38, 39; and EUR. PARL. DOC. PE 285.929, at 5–11 (2000). For the decision of the European Commision that approved the agreement, see Commission Safe Harbour Decision, *supra* note 102.

104 KUNER, *supra* note 76, at 185–87. For a highly negative assessment of the Safe Harbor Arrangement, see Joel R. Reidenberg, Essay, *The Simplification of International Data Privacy Rules*, 29 FORDHAM INT'L L.J. 1128, 1132–33 (2006). For a later discussion of the "substantial criticism of the Safe Harbor" by privacy supporters, see Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1975, 1986–87 (2005).

105 *See* Commission Safe Harbour Decision, *supra* note 102, annex III, at 26–30.

106 *See* Complaint, *In re* Google, Inc., FTC File No. 102-3136, Docket No. C-4336, at 6–8 (Oct. 13, 2011); Decision and Order, *In re* Google, Inc., FTC File No. 102-3136, Docket No. C-4336, at 3 (Oct. 13, 2011).

107 *See* Complaint, *In re* Facebook, Inc., FTC File No. 092-3184, Docket No. C-4365, at 17–18 (Nov. 29, 2011); Decision and Order, *In re* Facebook, Inc., FTC File No. 092-3184, Docket No. C-4365, at 3–4 (Aug. 10, 2012).

108 *See* DETERMANN, *supra* note 97, at 38.

109 In addition to participating in a safe harbor program, companies must also comply with local data collection rules, have a legitimate basis for the data transfer, and ensure that recipient companies afford an adequate level of data protection. *See id.* at 26–32.

110 Data Protection Directive, *supra* note 4, art. 26(2), at 46.

Model, pre-approved contractual clauses simplify the process of crafting data transfer agreements. Rather than use attorneys to draft contracts from scratch, a company can use the model contractual clauses and their "off-the-rack" language. Moreover, model declarations streamline the recognition by data protection commissions of internal privacy programs. Rather than having government agencies review and assess new contractual terms and conditions, companies can use terms and conditions that the EU already has found to provide adequate data protection. Large multinational entities had the most to gain from both the acceptance of Model Contractual Clauses and the Binding Corporate Rules, and in both policy areas, they played an important role in the discussions with the EU. A key part in the development of the second set of Model Contractual Clauses was played by the International Chamber of Commerce, a probusiness organization founded in 1919 with a secretariat located in Paris.[111]

The first set of Model Contractual Clauses was approved by the European Commission in 2001,[112] and the second set in 2004.[113] In the view of the Article 29 Working Party, contractual provisions are permissible only if they offer "satisfactor[y]" compensation for the absence of adequate data protection in the third country "by including the essential elements of protection which are missing in any particular situation."[114] Overall, these elements must offer reasonable compliance, redress, support, and other help to affected individuals.[115] The first set of model contractual clauses also contained a requirement of joint and several liability between the data exporter and data importer vis-à-vis the person whose personal data was transferred internationally.[116]

Due to the skepticism of international businesses toward these liability provisions, there was interest in development of another set

---

[111] For an analysis of the International Chamber of Commerce (ICC) Model Clauses, see Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 EUR. J. INT'L L. 441, 449 (2010). For a discussion by the ICC of its role in privacy law, see *Privacy and Personal Data Protection*, INT'L CHAMBER OF COMMERCE, http://www.iccwbo.org/Advocacy-Codes-and-Rules/Areas-of-work/Digital-Economy/Privacy-and-Personal-Data-Protection/ (last visited Mar. 30, 2013).

[112] Commission Decision 2001/497/EC, of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, under Directive 95/46/EC, 2001 O.J. (L 181) 19 [hereinafter Model Contractual Clauses 2001].

[113] Commission Decision 2004/915/EC, of 27 December 2004, Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74 [hereinafter Model Contractual Clauses 2004].

[114] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Working Document: Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries*, at 4, DG XV D/5005/98, WP 9 (Apr. 22, 1998).

[115] *Id.* at 4–11.

[116] Model Contractual Clauses 2001, *supra* note 112, annex, cl. 6(2), at 26.

of Model Contractual Clauses. The second framework makes each party liable for the damages that it causes.[117] The second Model Clauses contain a due diligence clause, however, that requires the exporter to guarantee that it will use "reasonable efforts" to determine that the importer would be able to satisfy all the contractual elements.[118] Both sets of Model Contractual Clauses are available for adoption by organizations.

(c) Binding Corporate Rules. — The EU has also permitted the use of Binding Corporate Rules as another way to meet the Directive's "adequacy" test. A basic aspect of Binding Corporate Rules is that they are available only when international data transfers occur within a single company or a group of affiliated companies.[119] These rules must allow enforcement by the affected individual (termed the "data subject" in EU privacy law), promise the corporation's cooperation with EU data protection authorities, and receive the approval of a data protection authority.

The Article 29 Working Party and national data protection commissioners played the key roles in the development of this policy instrument. In June 2003, the Article 29 Working Party declared Binding Corporate Rules to be an acceptable way to transfer data internationally within a corporate entity or group.[120] At that time, Binding Corporate Rules had to be approved by each local EU data protection authority whose country was implicated by the transfer.[121] This requirement meant that a company that intended to transfer personal information among its entities in France, Spain, Germany, and Poland would need the supervisory authorities in each of these countries to approve the identical corporate policy.

In January 2007, the Article 29 Working Party released a recommendation that streamlined this process.[122] It developed a standard application, a single form, intended to simplify the process of obtaining the approval of a data protection authority. Only a single copy of the form must be filled out, and this form can be submitted exclusively to a "lead" data protection authority.[123] The recommendation proposes a multifactor test for deciding which Member State's data protection au-

---

117 Model Contractual Clauses 2004, *supra* note 113, annex, cl. III(a), at 79.

118 *Id.* annex, cl. III(b), at 79.

119 DETERMANN, *supra* note 97, at 33.

120 Article 29 Data Protection Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, at 5–6, 11639/02/EN, WP 74 (June 3, 2003).

121 *See* KUNER, *supra* note 76, at 221.

122 Article 29 Data Protection Working Party, *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, WP 133 (Jan. 10, 2007).

123 *Id.* at 2–3 ("General Instructions").

thority is to be the lead one.[124] In June 2008, the Working Party released additional details regarding the preferred content and structure of Binding Corporate Rules.[125]

Even after the Working Party's release of these policy papers, the national data protection authorities continue to play the key role in approval of a Binding Corporate Rule — and some variations in approach remain at the national level. As Christopher Kuner notes, "most of the details of approval are determined" by the national authorities and each authority "has its own procedural rules for the approval of [Binding Corporate Rules]."[126] Companies that have gone through the approval process for these instruments include Accenture, BP, eBay, General Electric, HP, and Michelin.[127]

2. The Privacy Collision Averted. — These three policy instruments represent an impressive achievement; together they provide multiple means of avoiding a seemingly intractable difficulty. Recall that the Directive declared that personal data flows could pass to third countries only with adequate data protection, and that the EU was skeptical about the United States's level of privacy. In 1995, the combination of the adequacy standard and a data embargo power granted to national data protection commissioners in the EU created a risk of impeded global data exchanges.[128] As Professor Joel Reidenberg pointed out during this period: "If data protection is taken seriously, then systemic legal conflicts should cause disruption of international data flows."[129] Representative of the EU perspective on this potential conflict, in 1994 a leading European data protection expert stated: "[D]ata protection may be a subject on which you can have different answers to the various problems, but it is not a subject you can bargain about."[130] As Professor Gregory Shaffer observed in 2000, moreover, through the Directive, the EU member states were "pooling their sovereignty and acting collectively" in a fashion that "increased their

---

[124] *Id.* at 7 ("Common Application Part 1.3").

[125] Article 29 Data Protection Working Party, *Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules*, 1271-04-02/08/EN, WP 155 (June 24, 2008).

[126] KUNER, *supra* note 76, at 221.

[127] *List of Companies for Which the EU BCR Cooperation Procedure Is Closed*, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last visited Mar. 30, 2013).

[128] Schwartz, *supra* note 44, 488–92 (1995).

[129] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1337 (2000).

[130] Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 439 (1995) (quoting Spiros Simitis, Former Chair of the Council of Europe's Data Protection Experts Committee, Unpublished Comments at the Annenberg Conference on Information Privacy and the Public Interest (Oct. 6, 1994)).

influence" over information privacy policies throughout the world.[131] Yet something like bargaining did occur, and a privacy collision was averted.

Today, the Safe Harbor, Model Contractual Clauses, and Binding Corporate Rules permit international data transfers. Lothar Determann, a leading international privacy lawyer, concludes of these various compliance possibilities that "[a]lthough no one size fits all, most companies should be able to find a fitting size for each particular situation and development phase they are in."[132] Moreover, multinational companies have adopted these instruments as compliance benchmarks. These organizations use these compliance instruments to build EU-approved data protection standards and practices into their internal data processing operations.[133]

Two academic models regarding international policymaking provide a rich perspective on these negotiations in the shadow of the Directive. These are Anu Bradford's "Brussels Effect" and Anne-Marie Slaughter's "harmonization networks." This Article argues that the Brussels Effect has not occurred in this context. Two factors have proved significant in preventing such an effect: the existence of EU policies that sometimes conflict with information privacy and limits on the EU's power in the global information economy. In contrast, Slaughter's harmonization networks prove well represented in the context of global privacy policymaking and her scholarship permits a richer understanding of this process. Slaughter also develops a series of normative elements that help identify a future productive role for this disaggregated global web of policymakers.

(a) The Limits of the "Brussels Effect": Collaboration and Accommodation. — Bradford's "Brussels Effect" seeks to explain a widely observed phenomenon: the EU's ability to impose its rules throughout the world. Looking at the global power that the EU exercises through its institutions and laws, Bradford finds that the EU has successfully exported its standards in many legal and regulatory domains through de facto unilateralism.[134] Bradford uses the term "de facto" because states outside the EU remain formally bound only by their own legislation.[135] In the context of information privacy, however, only the "de facto" part of Bradford's de facto unilateralism seems accurate: the United States never enacted EU-style privacy legislation nor created EU-style institutions.

---

[131] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting of U.S. Privacy Standards,* 25 YALE J. INT'L L. 1, 87 (2000).

[132] DETERMANN, *supra* note 97, at 40.

[133] Bamberger & Mulligan, *supra* note 84, at 269–70.

[134] *See* Bradford, *supra* note 8, at 8.

[135] *See id.*

The examples that this Article has discussed of international "lawmaking" in the shadow of the Directive do *not* demonstrate the Brussels Effect. Rather, an EU-U.S. privacy collision was averted through a collaborative approach instead of through European unilateralism. This result is initially puzzling because the general conditions for the Brussels Effect appear to be present for information privacy. The absence of such an effect, and the legal paths that result from EU-U.S. cooperation, reveal important competing EU policy interests as well as the limits on the EU's power in a global information economy.

Bradford identifies a number of prerequisites that must be met before the Brussels Effect can occur in a given area of regulatory activity. For information privacy law, three such requirements are especially significant: EU nations must possess market power; the EU must have a specific regulatory capacity; and there must be "nondivisibility of standards," circumstances in which the objects of a regulation cannot easily use one set of standards inside the EU and another outside.[136]

These conditions for the Brussels Effect appear to exist for the processing of personal information. First, the EU is a rich consumer market that multinational companies cannot afford to avoid. As an affluent economic zone, it is also an important target for the kinds of consumer services and products that are at the cutting edge of the collection and processing of personal data.[137] Second, national data protection commissioners and EU government officials have a strong regulatory capacity for data protection.[138] The Directive itself heightened the EU's regulatory capacity in this area by requiring harmonizing legislation and the establishment in each member state of national data protection commissioners.[139]

---

[136] *Id.* at 17; *see id.* at 5, 10–19.

[137] On Europe's central role for American companies due to its sophisticated customers, see generally *Why Eurozone Woes Are Creating Headwinds for Global Firms*, KNOWLEDGE@WHARTON (Apr. 25, 2012), http://knowledge.wharton.upenn.edu/article.cfm?articleid=2986. As an example of the deep penetration of modern internet services in the EU, consider the great success of Facebook in Sweden (53.62% penetration, measured as the percentage of the population in the last month that uses Facebook), the UK (51.61%), Belgium (47.33%), the Netherlands (45.16%), and France (39.07%). In the United States, Facebook is at 52.56% penetration. *Facebook Statistics by Country*, SOCIALBAKERS, http://www.socialbakers.com/facebook-statistics/ (last visited Mar. 30, 2013).

[138] The Directive establishes the Article 29 Working Party, which consists of representatives of member states' national data protection authorities. Data Protection Directive, *supra* note 4, art. 29, at 48. Further regulatory capacity is provided by the Directive's establishment of a European Data Protection Supervisor (EDPS), an oversight authority for the EU's internal data processing operations. Beyond its formal mandate regarding the EU, the EDPS has taken a significant role in the global privacy debate. For an overview of the EDPS's many activities, see its homepage, EUR. DATA PROT. SUPERVISOR: THE EUR. GUARDIAN OF PERS. DATA PROT., http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en (last visited Mar. 30, 2013).

[139] *See* Data Protection Directive, *supra* note 4, art. 28, at 47–48.

Third, corporations' data privacy standards are likely to be nondivisible. Standards are nondivisible when a regulated entity prefers to adopt a single global standard rather than adopt a different standard for each jurisdiction in which it operates. Bradford writes: "[G]lobal standards emerge only when corporations voluntarily opt to comply with a single standard determined by the most stringent regulator, making other regulators obsolete in the process."[140] For example, as Bradford notes, U.S. companies face difficulties in isolating their databases exclusively for EU operations, and, hence, have adjusted "global operations to the most demanding EU standard."[141] This aspect of global database technology contrasts with labor markets, which are easily divisible.[142]

Thus, it appears that the conditions for a Brussels Effect are all in place for information privacy regulation. Yet the global policymaking process for information privacy has been more collaborative than unitary. It has been marked by negotiations among a wide variety of actors, and by concessions, sometimes considerable, from the EU. As the preceding section on post-Directive "lawmaking" has shown, there have been intermediate solutions negotiated between the United States and the EU, and in some cases, as in the second set of Model Contractual Clauses, between third parties and the EU. Moreover, legal inputs from the United States have made a difference in the negotiations and "lawmaking." There have been widespread contacts and government officials and private parties from the United States have engaged in discussion at all levels concerning the different elements and institutions of U.S. information privacy law.[143] In light of the Directive's strong assertion of EU authority over information flows, and in particular, in light of its grant to the EU's data protection commissioners of data embargo power, why did the EU engage in these multi-party negotiations? Why make concessions rather than uphold its requirements without compromise and rely on the market's Brussels Effect to export its rules? The answer, in short, is that the EU negotiated due to its own competing policy goals and because of the limits on its power in a global information economy.

The Directive itself embodies these competing policy goals. It seeks to protect information privacy as a human right, but it also en-

---

[140] Bradford, *supra* note 8, at 17.

[141] *Id.* at 18. Bradford specifically points to a "technical nondivisibility" in the area of information privacy. *Id.*

[142] To illustrate this point, Bradford notes that U.S. companies will not choose to use EU labor rules anywhere other than within EU member states. *Id.* at 18–19.

[143] As a recent example, a German-American Data Protection Day took place in May 2012 in Munich and featured Julie Brill, an FTC commissioner, as one of the speakers. Thomas Kranig, Editorial, *Ein angemessenes Datenschutzniveau — wer hat das wirklich?* [*An Adequate Level of Data Protection — Who Really Has It?*], 2012 ZEITSCHRIFT FÜR DATENSCHUTZ 245, 245–46.

deavors to promote trade and to permit a free flow of personal information. As this Article has discussed, one of the Directive's explicit goals is to facilitate the free flow of personal data within the EU. The Directive's Recital 56 states that "cross-border flows of personal data are necessary to the expansion of international trade."[144] Thus, the free flow of information, conditioned on adequate global data protection, was a key goal of the Directive.

At a deeper level, the EU has long been interested in the free flow of personal information and the trade in such data as part of the development of a vibrant internal market. The initial aim of the European Community's founding treaty was a common market, and in pursuit of this goal the EU has sought to protect free movement of goods, freedom to provide commercial and professional services, and free movement of capital.[145] The free flow of personal information is instrumental in achieving all of these tasks.

At the point where the internal market intersects with the global market, moreover, the EU faces a choice between liberalization and protectionism. This conflict has occurred in other areas of EU law;[146] in the context of privacy, it is noteworthy that the Directive itself requires "equivalent" standards of protection within the EU, but only "an adequate level of protection" from third party nations.[147] There is a long-standing and unresolved debate about the relationship between these standards.[148] Nonetheless, the choice of a mere adequacy standard for nonmember states acknowledges the benefits of a liberalized global trade in information. Transmissions of personal information outside of the EU lead to regulatory externalities and policy puzzles that are more complex than when information is merely shared between member states.

In 1993, the French data protection commission asked, "Do we want a Europe of merchants, or one of human rights?"[149] The answer to his rhetorical question is that the EU wants to have both. Indeed, as noted in the earlier section of this Article on the pre-Directive history, Europe has long sought both data trade and privacy protection. Here, I differ with Professor Joel Reidenberg, whose pathbreaking 2000 article posited a crisp dichotomy between the U.S. privacy ap-

---

144 Data Protection Directive, *supra* note 4, recital 56, at 36.

145 BERMANN ET AL., *supra* note 38, at 417.

146 *See, e.g.*, Bradford, *supra* note 8, at 55 (discussing the conflict between liberalization and protectionism in the area of food safety). *See generally* PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW 637–65 (4th ed. 2008).

147 Data Protection Directive, *supra* note 4, recital 8, at 32; *id.* art. 25(1), at 45.

148 Simitis, *supra* note 17, at 165.

149 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [NATIONAL COMMISSION ON INFORMATION TECHNOLOGY AND LIBERTIES], 14E RAPPORT D'ACTIVITÉ 1993 [14TH ACTIVITY REPORT 1993] 75 (1994).

proach and that in the EU. According to Reidenberg, U.S. information privacy regulation was based on liberal norms and market forces,[150] while the EU's information privacy regulations were based on "social-protection norms" according to which "data privacy is a political imperative anchored in fundamental human rights protection."[151] In my view, however, the lack of a Brussels Effect for data privacy, the resulting willingness to negotiate on the part of the EU, and the ensuing compromises point to a liberal, market-oriented approach *within* the EU.

There is a second factor behind the EU's use of a collaborative policymaking approach for data protection rather than reliance on the Brussels Effect. This factor rests on the strong desire of EU companies and consumers to access the global information economy. In this regard, one is reminded of a classic concept from legal positivism, the "normative power of the factual" (*normative Kraft des Faktischen*).[152] Cross-border flows have become an even more important part of international trade in the decades since the enactment of the Directive. Indeed, the large multinational companies involved in data trade, even if often founded outside the EU-zone, have quickly developed significant economic ties within the EU. In recognition of the importance of the information economy, Johannes Masing, a law professor and Justice on the Federal Constitutional Court of Germany, has noted the need for reasonable EU rules for international Internet companies and observed that "unhindered economic transactions are of the greatest importance for the future of Europe."[153]

Services and products of the information age have also proved highly popular among EU citizens. The release of the iPhone 5 provoked the same lines and excitement on September 21, 2012, in Munich, London, and Paris as it did in Berkeley, New York, and Chicago.[154] Facebook provides a further example in this regard with an

---

[150] *See* Reidenberg, *supra* note 129, at 1342–46.

[151] *Id.* at 1347.

[152] For background on this concept, see DIE NORMATIVE KRAFT DES FAKTISCHEN: DAS STAATSVERSTÄNDNIS GEORG JELLINEKS [THE NORMATIVE FORCE OF THE FACTUAL: GEORG JELLINEK'S UNDERSTANDING OF THE STATE] (Andreas Anter ed., 2004).

[153] Johannes Masing, *Herausforderungen des Datenschutzes* [*Challenges in Data Protection*], 2012 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 2305, 2310.

[154] For examples from the French and German press noting the consumer excitement, see *Débuts sans accrocs pour l'iPhone 5* [*Smooth Debut for the iPhone 5*], LES ECHOS (Sept. 21, 2012), http://m.lesechos.fr/tech-medias/debuts-sans-accrocs-pour-l-iphone-5-0202281974777.htm; Johannes Pennekamp, *Wir campen vor dem Apple-Store* [*We Camp in Front of the Apple Store*], FRANKFURTER ALLGEMEINE ZEITUNG (Sept. 21, 2012), http://www.faz.net/aktuell/wirtschaft/verkaufsstart-des-iphone-5-wir-campen-vor-dem-apple-store-11898193.html; and *iPhone-5-Fans stürmen deutsche Apple-Stores* [*iPhone 5 Fans Storm German Apple Stores*], FOCUS ONLINE (Sept. 21, 2012), http://www.focus.de/digital/handy/iphone/tid-27431/verkaufsstart-von-iphone-5-iphone-5-fans-stuermen-deutsche-apple-stores_aid_824234.html.

astonishingly high participation level in many EU countries.[155] A political skirmish over Facebook's privacy policy in the German state of Schleswig-Holstein also illustrates the centrality of information age services throughout the EU.

In the fall of 2011, the Independent State Center for Data Protection of Schleswig-Holstein published an expert opinion finding that Facebook's fan pages and its social plug-ins, such as the "like" button, violated various German data protection statutes, including the Telemedia Law (*Telemediengesetz* [*TMG*]).[156] Thilo Weichert, the Director of the center and Schleswig-Holstein's Data Protection Commissioner, requested that all private sector and public organizations in Schleswig-Holstein take down their Facebook fan pages and threatened to levy fines if no such action occurred.[157] Weichert also called upon the government of Schleswig-Holstein to remove its own Facebook fan page by October 31, 2011.[158] The government refused to do so — it chose Facebook over the stern recommendation of the Data Protection Commissioner.[159] A life without social media was as unthinkable for this state government as it is for millions of EU citizens.

In sum, there has not been a "unilateral regulatory globalization" of Brussels's privacy standards. Rather, the EU has been open to negotiated solutions in this area. In the next section, I consider the nature of these negotiations and of the entities that engaged in this process.

(b) "Harmonization Networks." — Anne-Marie Slaughter's scholarship presents an insightful perspective on global privacy policymaking. In contrast to Bradford's focus on the EU's unitary power, Slaughter's interest in *A New World Order* is on global governance through networks. She argues that the emerging "new world order" is "an intricate three-dimensional web of links between disaggregated

---

155 *See supra* note 137.

156 Feb. 26, 2007, BUNDESGESETZBLATT, Teil I [BGBL. I] at 179, art. 1 (amended 2010); *see Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook* [*Evaluation Under Data Protection Law of Web Analytics by Facebook*], UNÄBHANGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN [INDEPENDENT STATE CENTER FOR DATA PROTECTION OF SCHLESWIG-HOLSTEIN] 20–25 (Aug. 19, 2011), https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf.

157 *See* Press Release, Unäbhangiges Landeszentrum für Datenschutz Schleswig-Holstein [Independent State Center for Data Protection of Schleswig-Holstein], Bisher nur mäßiger Erfolg der ULD-Facebook-Abmahnungen [So Far Only Moderate Success for ULD's Facebook Warnings] (Nov. 4, 2011), *available at* https://www.datenschutzzentrum.de/presse/20111104-facebook-abmahnungen.htm.

158 *See* Press Release, Landesregierung Schleswig-Holstein [Schleswig-Holstein State Government], Datenschutz Facebook: Staatssekretär Dr. Wulff will Fan-Page Schleswig-Holstein nicht abschalten [Facebook Data Protection: Secretary of State Dr. Wulff Does Not Intend to Shut Down Schleswig-Holstein's Facebook Page] (Oct. 31, 2011), *available at* http://www.schleswig-holstein.de/ArchivSH/PI/STK/2011/CdS/111031_stk_cds_facebook.html.

159 It merely added a warning to its page that clicking on the "like" button on the fan page would lead to information being shared with Facebook. *Id.*

state institutions."[160] In Slaughter's estimation, states now relate to each other through their parts and not through their whole. States are "disaggregated," that is, they interact not only through their foreign offices and state departments, but also through a variety of regulatory, judicial, and legislative channels.[161]

An important part of these disaggregated interactions occurs through "harmonization networks."[162] These networks emerge from the actions of regulators working "within the framework of a trade agreement, often with a specific legislative mandate . . . to harmonize regulatory standards . . . with the overt aim of achieving efficiency."[163] In this sense, "harmonization" is the process by which these ad hoc groups adjust the regulatory standards of multiple countries to achieve a mutually acceptable outcome. As Slaughter writes, "The more that international commitments require the harmonization or other adjustment of domestic law, the coordination of domestic policy, or cooperation in domestic enforcement efforts, the more they will require government networks to make them work."[164] Harmonization networks can also generate distinct mechanisms for compliance within each nation.

Slaughter's scholarship helps explain the nature of the cooperative lawmaking that occurred in the shadow of the EU Data Protection Directive. Notably, a wide variety of ad hoc networks emerged after 1995 to adjust and develop EU and U.S. law and make possible compliance with the Directive. Indeed, this harmonization took place in an even more ad hoc fashion than Slaughter foresees. It did not occur within the formal framework of an EU-U.S. trade or treaty agreement, but as a series of policy improvisations following the EU's enactment of the Directive.

The harmonization networks of data protection law have also involved a disparate group of participants. In the EU, important roles have been played by the Commission, Council of Ministers, Parliament, Article 29 Working Group, European Data Protection Supervisor, Berlin Group on Telecommunications and Data Protection, and national and state data protection supervisors.[165] Non-EU parties in-

---

160 SLAUGHTER, *supra* note 9, at 15.

161 *Id.* at 5.

162 *Id.* at 20.

163 *Id.* at 59.

164 *Id.* at 162.

165 As an example of these networks in action, the national data protection commissioners issue regular policy statements at the conclusion of each annual Data Protection Conference. The 2012 Conference was held in Uruguay and led to declarations about cloud computing, "the future of privacy," and profiling. *Resolutions and Declaration Adopted*, 34TH INT'L CONFERENCE OF DATA PROT. AND PRIVACY COMM'RS (2012), http://www.privacyconference2012.org/english/sobre-la-conferencia/noticias/Resoluciones+y+declaraciones+adoptadas.

volved in the "lawmaking" have included the U.S. Commerce Department and the FTC, which now has full member status at the annual meeting of the world's data protection commissioners and its own high level contacts with EU officials that work on privacy-related issues.[166] As noted earlier, the FTC has enforced the Safe Harbor Agreement with the EU against Facebook and Google.[167] That enforcement is a fascinating example of collaborative lawmaking between the EU and the United States with the content of norms developed by the two legal systems and then enforced by one side. U.S. privacy advocacy groups, such as the Electronic Privacy Information Center, have participated in hearings at the European Parliament and in discussions at the OECD's Working Party on Information Security and Privacy.[168]

Finally, when building blocks for policymaking are disaggregated parts of states, there are possible dangers. The risk is "an end run around the formal constraints — representation rules, voting rules, and elaborate negotiating procedures — imposed on global governance by traditional international organizations."[169] Slaughter warns, "Existing networks breed suspicion and opposition in many quarters, leading to charges of technocracy, distortion of global and national political processes, elitism and inequality."[170] In response to these risks, Slaughter points to a need for a transformation of harmonization networks through attention to a handful of important norms and proposed elements.[171] Perhaps the three most promising for the future of global privacy policymaking are subsidiarity, checks and balances, and enhancements to the accountability of government networks. I return to these proposals later in this Article when I consider necessary modifications to the Proposed Regulation.

III. THE EU'S PROPOSED DATA PROTECTION REGULATION

In January 2012, the EU released its Proposed General Data Protection Regulation.[172] This document marks an important policy shift from directives to regulations. In EU law, while a directive requires harmonizing legislation, a regulation establishes directly enforceable

---

166 32nd Int'l Conference of Data Prot. and Privacy Comm'rs, *Accreditation Resolution* (2010), *available at* http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26497/Accreditationresolution.pdf; *see supra* p. 1980.

167 *See supra* p. 1981 and sources cited notes 106–107.

168 For an example of testimony by Marc Rotenberg, President of the Electronic Privacy Information Center, before the European Parliament, see *EPIC Urges Support for New European Privacy Framework*, ELECTRONIC PRIVACY INFO. CENTER (Oct. 9, 2012), http://epic.org/2012/10/epic-urges-support-for-new-eur.html.

169 SLAUGHTER, *supra* note 9, at 28.

170 *Id.* at 266.

171 *Id.* at 29–30.

172 *Proposed Regulation*, *supra* note 3.

standards. As Kuner explains, "a regulation leads to a greater degree of harmonization, since it immediately becomes part of a national legal system, without the need for adoption of separate national legislation; has legal effect independent of national law; and overrides contrary national laws."[173]

Two developments are responsible for this shift in policy. First, in 2010, the Commission had already pointed to the "new challenges for the protection of personal data" created by "rapid technological developments and globilisation."[174] Technology allowed "ways of collecting personal data [to] become increasingly elaborated and less easily detectable."[175] Second, technology made more personal information "publicly and globally available on an unprecedented scale."[176]

In light of these two challenges, the Directive fell short, and the Commission did not mince words in noting the lack of sufficient harmonization of data protection throughout the EU. For example, member states were interpreting the rules for consent differently,[177] and the Directive's grant of "room for manoeuvre in certain areas" and its permitting member states to issue "particular rules for specific situations" had created "additional cost[s] and administrative burden[s]" for private stakeholders.[178] Due to this absence of uniformity under the Directive, a regulation was needed to create legal certainty within the internal market and to assure a continuing role for the EU "in promoting high data protection standards worldwide."[179]

The resulting policy instrument, the Proposed Data Protection Regulation, has contradictory tendencies. To express its spirit, one might quote Walt Whitman: "I contradict myself; I am large . . . . I contain multitudes."[180] The Proposed Regulation offers varied possibilities: it has the potential both to destabilize the current status quo between the EU and United States and to build on the current approach by creating new paths for accommodation between the two systems.

---

[173] Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, 11 PRIVACY & SECURITY L. REP. 215, 217 (2012).

[174] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions*, at 2, COM (2010) 609 final (Nov. 11, 2010) [hereinafter *2010 Communication*] (emphasis omitted).

[175] *Id.* (emphasis omitted).

[176] *Id.*

[177] *Id.* at 8.

[178] *Id.* at 10.

[179] *Id.* at 5; *see also id.* at 16. The lack of uniformity under a directive is a larger phenomenon of EU law, and has been identified in other regulatory contexts. *See, e.g.*, Katerina Linos, *How Can International Organizations Shape National Welfare States? Evidence from Compliance with European Union Directives*, 40 COMP. POL. STUD. 547, 562 (2007).

[180] WALT WHITMAN, LEAVES OF GRASS 55 (1855).

A. Destabilization of the Equilibrium

The Proposed Regulation carries a potential for destabilization of the current status quo. It adds additional protections for individual rights beyond those in the Directive. These protections strengthen existing requirements for data minimization and for the legal standard an organization must satisfy before processing personal information. The Proposed Regulation also develops a controversial "right to be forgotten"[181] and elaborates stricter requirements before "consent" can be used as a justification for data processing.[182] There is a further emphasis on the unique EU categories of protection from automated processing[183] and from use of sensitive data.[184] These aspects of the Proposed Regulation create greater distance between the EU and U.S. systems for information privacy law and cast the current status quo into doubt. The Proposed Regulation also destabilizes institutional relations *within* the EU. It significantly increases the power of the Commission and takes power away from the member states and national data protection commissions.[185]

1. Heightened Individual Rights. — As an initial step in strengthening individual rights, the Proposed Regulation heightens existing EU requirements for a legal basis before an organization engages in data processing. Its Article 5 states that personal data "shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data."[186] Recital 30 states more broadly, "[p]ersonal data should only be processed if the purpose of the processing could not be fulfilled by other means."[187] Even if such a general basis for data processing exists, there is a further requirement of data minimization. Article 5 requires personal data to be "adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed."[188] Firms also may not process data "in a way incompatible" with their original collection, which is to be "for specified, explicit and legitimate purposes."[189]

The Proposed Regulation thus only allows organizations to process personal data for limited and specified purposes. It also imposes tem-

---

181 *Proposed Regulation*, *supra* note 3, art. 17, at 51.

182 *Id.* art. 7, at 45.

183 *Id.* art. 2, at 40–41.

184 *Id.* art. 9, at 45–46.

185 In fact, the "Legislative Financial Statement" at the end of the Proposed Regulation classifies the "Management Mode" of the regulation as "Centralised direct management by the Commission." *Id.* at 101–07.

186 *Id.* art. 5(c), at 43.

187 *Id.* recital 30, at 22.

188 *Id.* art. 5(c), at 43.

189 *Id.* art. 5(b), at 42.

poral limits on data use. As part of this approach, the Proposed Regulation creates the newfound "right to be forgotten."[190] Within the academy, Professor Viktor Mayer-Schönberger has been a leading proponent of the deletion of personal information to protect privacy.[191] The Proposed Regulation dedicates an article to this interest, which it links to a right "to erasure."[192] Of the right to be forgotten, the Proposed Regulation states, "The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data" should a number of conditions apply.[193]

The "right to be forgotten" has significant potential for creating conflict with the United States. Indeed, even within the EU, this interest also raises difficulties regarding the necessary balance of privacy against the freedom of expression and historical research. For example, the Proposed Regulation places the responsibility on the "controller" of the information to inform third parties of the duty to erase data.[194] Consistent with long-established EU data protection law, the Proposed Regulation defines a controller as the person or entity that "determines the purposes, conditions and means of the processing of personal data."[195] The right to be forgotten raises complex questions regarding the precise obligations of the controller and downstream third parties, such as search engines and advertising networks, which have many innovative ways of collecting, tracking, and, in some cases, reidentifying data.[196]

The Proposed Regulation strengthens individual rights in other ways. Among the most important of these measures are those that heighten existing consent requirements. As Kuner observes, consent is an especially important concept in the EU because it is in "widespread use . . . as a legal basis for data processing."[197] The Proposed Regulation reinforces the Directive's concept of consent by placing "the burden of proof" on a "controller" to show that individuals agree to the processing of their personal data.[198] The Proposed Regulation also de-

---

[190] *Id.* art. 17, at 51–53.

[191] *See generally* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

[192] *Proposed Regulation*, *supra* note 3, art. 17(1), at 51.

[193] *Id.* These conditions include: "the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"; consent for the processing has been withdrawn; the authorized storage period has expired; or the concerned individual has objected to the processing of the information. *Id.* art. 17(1)(a)–(d), at 51.

[194] *Id.* art. 17(2), at 51.

[195] *Id.* art. 4(5), at 41.

[196] On these processes, see Jennifer Valentino-DeVries & Jeremy Singer-Vine, *They Know What You're Shopping For*, WALL ST. J., Dec. 8, 2012, at C1.

[197] Kuner, *supra* note 173, at 220.

[198] *Proposed Regulation*, *supra* note 3, art. 7(1), at 45.

clares that "[c]onsent shall not provide a legal basis for [data] processing, where there is a significant imbalance between the position of the data subject and the controller."[199] These provisions reflect a skepticism in the EU as to how volitional consent truly is.[200]

Further, the Proposed Regulation heightens the protections of the Directive for sensitive data and strengthens existing restrictions on automated decisionmaking. Article 9 provides a list of kinds of sensitive data, which it terms "special categories of personal data."[201] Following the Directive's approach, Article 9 flatly forbids the processing of "special categories" unless one of its specific exceptions is applicable.[202] The EU's attention to its "special categories" does not focus on risks from specific data processing operations, but singles out areas as being ex ante problematic for data processing. The Information Commissioner's Office in the United Kingdom has already criticized the Proposed Regulation's provisions for sensitive data due to "the inflexible nature of the grounds on which such data can be processed."[203] In addition, the Proposed Regulation's exceptions to its general ban on processing are drafted in a narrow fashion that may prove unworkable.

As for automated processing, the Proposed Regulation ties this concept to more contemporary concerns about profiling. Article 20 is worth quoting at length:

> Every natural person shall have the right not to be subject to a measure . . . which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.[204]

By increasing the Directive's protections for personal data, the Proposed Regulation threatens certain contemporary forms of "automated processing," most notably analytics. I return to this topic in section III.C.1.

---

[199] *Id.* art. 7(4), at 45.

[200] *See* Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*, at 2, 01197/11/EN, WP 187 (July 13, 2011) (warning that if consent is "incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing"); *see also* Spiros Simitis, *§ 4a — Einwilligung*, *in* KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ, *supra* note 17, at 432, 435 (warning that "consent" becomes a mere fiction if the affected party does not have a real possibility of influencing how his or her personal information is used).

[201] *Proposed Regulation*, *supra* note 3, art. 9, at 45.

[202] *Id.* art. 9(1)–(2), at 45–46.

[203] *Initial Response from the ICO on the European Commission's Proposal for a New General Data Protection Regulation*, INFO. COMMISSIONER'S OFF. (Jan. 25, 2012), http://www.ico.gov.uk/news/latest_news/2012/statement-initial-response-new-data-protection-regulation-proposals-25012012.aspx.

[204] *Proposed Regulation*, *supra* note 3, art. 20(1), at 54.

Finally, the Proposed Regulation increases the protection of individual rights by greatly increasing the size of monetary sanctions that are available for violations of them. Overall, these fines are to be "effective, proportionate and dissuasive."[205] Article 79 sets out a multifactor test for calculation of administrative fines by national data protection commissioners. It states:

> The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented [as part of data protection by design] . . . and the degree of cooperation with the supervisory authority in order to remedy the breach.[206]

This test provides a great measure of flexibility for the individual data protection commissioner in assessing penalties in individual cases. Of special note, moreover, the Proposed Regulation permits fines under certain circumstances to reach as much as two percent of a company's worldwide revenues.[207] At least on paper, this provision would seem to permit penalties of as much as several hundred million dollars against large technology companies.[208] A fine of such magnitude might run afoul, however, of the Regulation's requirement that fines be "proportionate."[209] Nonetheless, these penalty provisions demonstrate the EU's firm intention of ensuring compliance with its data protection rules by the global technology companies that process personal data.

2. A Centralization of Regulatory Power. — Although I have begun my discussion of the Proposed Regulation with its protection of rights, much of that document concerns the organization and practice of data protection within the EU. As Professor Gerrit Hornung has noted: "Institutional and organizational arrangements make up a significant part of the draft."[210] Some of these measures have been received with general approval, such as the steps that the Proposed Regulation takes to guarantee the independence of data protection commissions within their member states.[211] Yet the Proposed Regulation also contains

---

[205] *Id.* art. 79(2), at 92.

[206] *Id.*

[207] *Id.* art. 79(6), at 93.

[208] Kuner, *supra* note 173, at 226.

[209] *Proposed Regulation*, *supra* note 3, art. 79(2), at 92.

[210] Gerrit Hornung, *Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012* [A Fundamental Data Protection Regulation for Europe? Light and Shadow in the Commission Draft of January, 25, 2012], 2012 ZEITSCHRIFT FÜR DATENSCHUTZ 99, 104.

[211] *See, e.g.*, INFO. COMM'R'S OFFICE, INITIAL ANALYSIS OF THE EUROPEAN COMMISSION'S PROPOSALS FOR A REVISED DATA PROTECTION LEGISLATIVE FRAMEWORK 22 (2012), *available at* www.ico.gov.uk/~/media/documents/library/Data_Protection

controversial measures that destabilize the organizational status quo: first, it creates a "consistency mechanism,"[212] and, second, it grants power to the Commission to create a wide range of "delegated" and "implementing" acts.[213] One analysis of the Proposed Regulation has found that it identifies forty-five different areas that can be regulated through such acts.[214] The result centralizes data protection decision-making in the Commission.

The impact of these steps on privacy subsidiarity within the EU is significant, and the reaction within the EU regarding these aspects of the Proposed Regulation has been strongly negative. In Germany, the Bundesrat, or Federal Council, which represents the sixteen states of Germany in the federal legislative process, issued a resolution objecting to the Proposed Regulation.[215] It declared that the Proposed Regulation engages in an "almost complete displacement of the data protection rules in member states."[216] In France, the National Commission on Information Technology and Liberties objected to the regulation as "a centralization of the regulation of private life for the benefit of a limited number of authorities, and equally for the benefit of the Commission, which will gain an important normative power."[217] It also pointed to aspects of the Regulation that would reinforce the "bureaucratic and distant image of community institutions" and reduce the status of data protection commissioners to that of a "mailbox" for passing on complaints to other authorities.[218]

Commentators have also wondered whether the Regulation violates "subsidiarity," a key tenet of EU law. Alexander Dix, the Berlin Data Protection Commissioner, argues that "the powers that the Commission grants itself in this process go far beyond the permissible."[219] A long-standing advocate of the "modernization" of EU data protection, Professor Alexander Roßnagel nonetheless finds the Proposed Regula-

---

/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx ("We welcome the explicit requirement that data protection supervisory authorities shall be completely independent and properly resourced.").

212 *Proposed Regulation*, *supra* note 3, art. 57, at 82.

213 *Id.* art. 86, at 97–98; *id.* recitals 129–32, at 37–38.

214 Alexander Dix, *Datenschutzaufsicht im Bundesstaat — ein Vorbild für Europa* [*Data Protection Oversight in the Federal State — A Model for Europe*], 36 DATENSCHUTZ UND DATENSICHERHEIT 318, 321 (2012).

215 BUNDESRAT DRUCKSACHEN [BR] 52/1/12 (Ger.).

216 *Id.* at 2.

217 *Projet de règlement européen: la défense de la vie privée s'éloigne du citoyen* [*Proposed European Regulation: Defense of Private Life Moves Away from Citizens*], COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) (Jan. 26, 2012), http://www.cnil.fr/la-cnil/actualite/article/article/projet-de-reglement-europeen-la-defense-de-la-vie-privee-seloigne-du-citoyen-1/.

218 *Id.*

219 Dix, *supra* note 214, at 321.

tion to represent the wrong kind of reform. He criticizes it as a "highly radical solution" that is based on a "centralized and monopolized regulation."[220] Relatedly, commentators have also argued that the Proposed Regulation violates not only the EU principle of subsidiarity, but also that of proportionality. Subsidiarity requires decentralized governance in the EU; proportionality is a means-end test that evaluates whether a measure is appropriate and necessary to achieve a legislative goal.[221]

The first step that the Proposed Regulation takes to centralize power at the EU is its "consistency mechanism." The Proposed Regulation creates a new institution, the European Data Protection Board (EDPB).[222] In so doing, the Proposed Regulation upgrades the status of the Article 29 Working Party, the panel of national supervisory authorities.[223] The EDPB provides a useful forum in which national supervisory authorities can reach a consensus about important issues. The role of these national officials is a long-established one. As Professor Abraham Newman argues, governmental officials in individual countries with data protection legislation, in particular France, Germany, and the United Kingdom, played a central role throughout the 1980s and 1990s in the creation of supranational privacy protection in Europe.[224] Drawing on their important "vertical ties,"[225] data protection commissioners in EU nations with existing legislation acted as "transgovernmental policy entrepreneurs" through the drafting of the Directive and afterwards.[226]

The EDPB offers a new institutional framework for drawing on these important ties. While the EDPB permits each national data protection commission to make final regulatory choices, it requires a draft proposal to be filed with it and the European Commission before a national commission can adopt a measure relating to certain kinds of

---

[220] Alexander Roßnagel, Editorial, *Datenschutzgesetzgebung: Monopol oder Vielfalt?* [*Data Protection Legislation: Monopoly or Diversity?*], 36 DATENSCHUTZ UND DATENSICHERHEIT 553, 553 (2012).

[221] *See, e.g.*, Michael Ronellenfitsch, *Fortentwicklung des Datenschutzes: Die Pläne der Europäischen Kommission* [*Further Development of Data Protection: The Plans of the European Commission*], 36 DATENSCHUTZ UND DATENSICHERHEIT 561, 562–63 (2012); Hans-Hermann Schild & Marie-Theres Tinnefeld, *Datenschutz in der Union — Gelungene oder missglückte Gesetzentwürfe?* [*Data Protection in the Union — Successful or Unsuccessful Draft Legislation?*], 36 DATENSCHUTZ UND DATENSICHERHEIT 312, 316 (2012). For a general discussion of the importance of subsidiarity and proportionality in EU law, see CRAIG & DE BÚRCA, *supra* note 146, at 100–04.

[222] *Proposed Regulation*, *supra* note 3, arts. 64–72, at 86–89.

[223] *See id.* art. 64, at 86 (providing that the EDPB will be composed of "the head of one supervisory authority of each Member State and of the European Data Protection Supervisor").

[224] NEWMAN, *supra* note 96, at 88–89.

[225] *Id.* at 92.

[226] *Id.* at 98.

matters. The prefiling requirement extends to matters affecting information processing in several member states, international data transfers, and a variety of other topics.[227] The EDPB's subsequent nonbinding recommendations will be valuable to the process of developing consensus about important transnational privacy issues among all member states. The EDPB will offer an opinion on a matter by simple majority.[228] The national data protection authority will then "take account of the opinion" and, within two weeks, notify the EDPB and the Commission "whether it maintains or amends its draft measure."[229]

More controversially, the Proposed Regulation grants great power to the European Commission. It gives the Commission the authority under the consistency process to issue opinions to "ensure correct and consistent application" of the Regulation.[230] At an initial stage, the national data protection authority must "take utmost account of the Commission's opinion."[231] Additionally, the Commission may require national data protection authorities "to suspend the adoption" of a contested draft measure.[232] Thus, through the "consistency process," the Proposed Regulation grants the Commission the final word on a wide range of matters concerning the interpretation and application of the Proposed Regulation throughout the EU and beyond.

The Proposed Regulation also assigns the Commission the power to adopt "delegated acts" and "implementing acts" under a wide range of circumstances. Delegated acts supplement or amend nonessential elements of EU legislation, and implementing acts enact procedures to put the legislation into effect. The Proposed Regulation contains numerous grants of power to adopt both kinds of acts, plus a general grant in Article 62(1) to issue implementing acts to decide "on the correct application" of the Regulation under almost limitless circumstances.[233] As Kuner concludes, the result is "a substantial shifting of power regarding data protection policymaking from the EU member states and the [data protection authorities] to the Commission."[234] There has been an outcry against delegated and implementing acts as demonstrated by leaked comments dated July 18, 2012, from member

---

[227] *See Proposed Regulation*, *supra* note 3, art. 58(1)–(2), at 82–83.

[228] *Id.* art. 58(7), at 83.

[229] *Id.* art. 58(8), at 83.

[230] *Id.* art. 58(4), at 83.

[231] *Id.* art. 59(2), at 84. If the national supervisory authority neglects to follow the opinion of the Commission, it is required to "inform the Commission and the European Data Protection Board . . . and provide a justification." *Id.* art. 59(4), at 84.

[232] *Id.* art. 60(1), at 84.

[233] *Id.* art. 62(1), at 85; *see id.*

[234] Kuner, *supra* note 173, at 227.

states to the Council of the EU.[235] The national delegations of France, Germany, Italy, Luxembourg, Norway, Poland, Sweden, and the United Kingdom all objected to this aspect of the Proposed Regulation.[236]

B. Paths to Accommodation

At the same time that the Proposed Regulation destabilizes the current policy equilibrium, it offers paths toward a new balance. This new direction begins with international collaboration. The Proposed Regulation also consolidates the results of previous negotiations about international data flows and introduces privacy and security innovations from around the world into EU law. Thus, the Proposed Regulation builds on the Directive's achievements and points the way forward to continuing international policymaking.

First, Article 45 of the Proposed Regulation sets out an aspirational call for collaboration in data protection among European officials, national regulators, and nongovernmental organizations. This work is to include development of "effective international co-operation mechanisms"; provision of "international mutual assistance in the enforcement of legislation"; engagement of "relevant stakeholders in discussion and activities"; and promotion of "the exchange and documentation of personal data protection legislation and practice."[237] Through these provisions, the Proposed Regulation envisions a world of cross-fertilization of ideas, mutual assistance, and, through its idea of "co-operation mechanisms," possible new forms of institutional relations.

Second, the Proposed Regulation consolidates many of the policies negotiated post-Directive. In particular, the Proposed Regulation acknowledges the validity of the Safe Harbor Agreement, Binding Corporate Rules, and contractual clauses. Its Articles 41(8) and 42(5) confirm that decisions of the Commission and of the data protection authorities of member states will remain in force once the Directive is repealed.[238] As a result, the Safe Harbor Agreement will be valid un-

---

[235] Note from Gen. Secretariat to Working Grp. on Info. Exch. & Data Prot., Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (July 18, 2012), *available at* http://www.statewatch.org/news/2012/jul/eu-council-dp-reg-ms-positions-9897-rev2-12.pdf.

[236] For these objections to the delegated and implementing acts in the note from General Secretariat, see *id.* at 54 (France); *id.* at 25 (Germany); *id.* at 73 (Italy); *id.* at 90 (Luxembourg); *id.* at 166 (Norway); *id.* at 101 (Poland); *id.* at 130 (Sweden); and *id.* at 138 (United Kingdom).

[237] *Proposed Regulation*, *supra* note 3, art. 45(1)(a)–(d), at 74. The Proposed Regulation also requires the EDPB to encourage "the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide." *Id.* art. 66(1)(g), at 87.

[238] *See id.* arts. 41(8), 42(5), at 70–71.

der the Proposed Regulation. As for Binding Corporate Rules, the Proposed Regulation sets out the means for their approval in Article 43.[239] This proposal largely adopts the requirements that the Article 29 Working Party has established for these policy instruments. Moreover, the Proposed Regulation permits international transfers of data through model contractual clauses, now termed "standard data protection clauses," as well as contractual clauses for specific transfers that have been approved by a data protection authority.[240]

Third, the Proposed Regulation incorporates a number of privacy policy innovations, some of which have roots outside of the EU. In 1995, the Directive had demonstrated a willingness to absorb policy innovations made *within* the EU. The Proposed Regulation proves similarly willing to absorb recent information privacy policy innovations, whether from EU member states or elsewhere. By incorporating these innovations, the Proposed Regulation demonstrates its openness to the work of global policy entrepreneurs. Among the privacy regulatory innovations that the Commission incorporated into the Proposed Regulation are data breach notifications; data protection impact assessments; data protection by design; and the concept of "responsibility," which has more typically been termed "accountability."[241] The last concept provides an especially interesting example of privacy policy entrepreneurship.

The OECD's Privacy Guidelines contain an early, if underdeveloped, mention of accountability. The OECD Guidelines require the "data controller" to "be accountable for complying with" their principles.[242] More recently, a joint policymaking effort has sought to create standards of accountability for the twenty-first century.[243] This project has been facilitated by a U.S. organization, the Centre for Information Policy Leadership, and began with the Irish Data Protection Commissioner's multiyear "Galway Project."[244] These initial steps have been followed by accountability projects led by the French data

---

[239] *See id.* art. 43, at 71–73.

[240] *Id.* art. 42(2)(b)–(d), at 70–71.

[241] *Id.* arts. 31, 32, at 60–62 (data breach notifications); *id.* art. 33, at 62–63 (data protection impact assessments); *id.* art. 23, at 56 (data protection by design); *id.* (accountability).

[242] OECD Guidelines, *supra* note 23, art. 14.

[243] CTR. FOR INFO. POLICY LEADERSHIP, HUNTON & WILLIAMS LLP, DATA PROTECTION ACCOUNTABILITY: THE ESSENTIAL ELEMENTS 6 (2009), *available at* http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

[244] *See id.* at 3.

protection commissioner[245] and a resolution on the topic issued in 2009 by EU data protection commissioners in Madrid.[246]

As a policy idea, the accountability principle focuses on whether a data processing entity has created internal processes that are commensurate to potential data threats.[247] It represents an effort to move away from the creation of formalistic, top-down obligations for data processors, such as a requirement to file declarations with national data protection commissioners. The Proposed Regulation's Article 22 offers a positive response to the revival of this concept.[248] It places an obligation on the "controller" to demonstrate compliance with the Proposed Regulation by adopting both internal policies and "mechanisms to ensure the verification of the effectiveness" of the resulting measures.[249]

C. Averting the Privacy Collision Ahead: A Turn to Procedures and Institutions

What then is the prognosis for life under the Proposed Regulation? In 1995, with the Directive staking out positions that permitted data embargoes and pointed to future international conflict, Professor Fred Cate noted that "all of the affected parties recognize the important opportunity presented by the Directive for meaningful consultations between U.S. and European business and government leaders."[250] These consultations occurred; even more so, creative "lawmaking" took place through networks of government officials and private citizens engaged in policy entrepreneurship. Here is Slaughter's EU as a "vibrant laboratory" — and a laboratory open to participation by a wide cast.[251]

In assessing the potential privacy collision under the Proposed Regulation, this Article considers the kinds of institutions and procedures that can make future collaborative "lawmaking" possible in the shadow of a new EU policy instrument. Here, I wish also to assess the

---

[245] *See* CTR. FOR INFO. POLICY LEADERSHIP, HUNTON & WILLIAMS LLP, DEMONSTRATING AND MEASURING ACCOUNTABILITY: ACCOUNTABILITY PHASE II — THE PARIS PROJECT (2010), *available at* http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.pdf.

[246] *International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution,* INT'L CONF. OF DATA PROTECTION AND PRIVACY COMMISSIONERS (Nov. 5, 2009), http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

[247] CTR. FOR INFO. POLICY LEADERSHIP, *supra* note 243, at 8–9.

[248] *See Proposed Regulation*, *supra* note 3, art. 22, at 55–56.

[249] *Id.* art. 22(1), at 55 (directing the adoption of internal policies); *id.* art 22(3), at 55 (verification mechanisms).

[250] Cate, *supra* note 130, at 442. Cate also noted that the Directive "threatens U.S. leadership in the information economy and is heightening U.S. concern over protecting that so-called dominance." *Id.* at 440.

[251] SLAUGHTER, *supra* note 9, at 264.

value of subsidiarity, checks and balances, and the accountability and transparency of government networks. These ideas, found among Slaughter's normative suggestions for harmonization networks, also reflect important concepts in EU law.

1. Subsidiarity. — Subsidiarity is a cornerstone of EU law. Jean Monnet, one of the intellectual founders of the EU, emphasized the value of locating governmental power at the lowest level practicable. The idea is enshrined in the Treaty on European Union's Article 5, which also includes a concept of proportionality.[252] The Lisbon Treaty of 2007 strengthens subsidiarity by giving national parliaments a direct role in enforcing it.[253] In her theory of harmonization networks, Slaughter also points to this concept as an important element in the success of a disaggregated policy process.[254]

What are the lessons of subsidiarity for life under the Proposed Data Protection Regulation? An optimal outcome to the consultation process now underway at the EU would reduce the scope of the Proposed Regulation. The Proposed Regulation creates binding law for member states in a way that occupies too many areas, sweeps too broadly, and leaves too little room for future policy experiments. Regarding the scope of the resulting revised regulation, the EU should limit it to key definitional concepts, or "field definitions." Such definitions are basic conceptual categories that mark a regulatory field.[255] The field definitions in a revised regulation should develop EU-wide concepts for the term "personal information," the elements of consent, the jurisdictional bases for transnational application of EU privacy standards, and the formal requirements for data protection commissions. As a final definitional matter, a revised regulation should set out the requirements for an EU Data Protection Commission, a topic that I address in the next section.

By marking the scope of these regulatory fields, a revised regulation would encourage uniformity in basic elements of EU data protection law and reduce regulatory transaction costs on an international scope. It would also permit room for further experiments, which is a key benefit of subsidiarity. For example, consider the heightened individual rights under the Proposed Regulation. The need is for harmonization networks to develop innovative ways to interpret and apply these interests consistent with an international free flow of information. These loosely aggregated networks of government officials

---

[252] Consolidated Version of the Treaty on European Union art. 5(1), May 9, 2008, 2008 O.J. (C 115) 13, 18.

[253] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities protocol A, Dec. 17, 2007, 2007 O.J. (C 306) 1, 148.

[254] SLAUGHTER, *supra* note 9, at 259.

[255] For an earlier use of the term "field definitions," see Schwartz, *supra* note 57, at 942.

and private individuals can lead to a cross-fertilization of policy models and can help devise ways to comply with the Proposed Regulation's new rules for cross-border data flows.

The principle of subsidiarity also suggests a path for innovative regulatory responses to one of the most promising contemporary forms of "automated" processing, namely analytics. Through analytics, organizations take information that they have or to which they can gain access and convert it to actionable knowledge.[256] Among nonconsumer uses of this technology, analytics play an important role in health care research, data security, and fraud prevention. Yet the EU appears to regulate and limit analytics even at those initial stages when data are collected, integrated, and analyzed. Under EU law, these steps are likely to constitute a processing of data that has a "legal effect" on a person under EU law.[257] In this fashion, the Proposed Regulation creates a potential threat to socially productive uses of analytics — including ones that may not raise significant risks of individual privacy harms. There is a need for innovative, multistakeholder discussions around accountability to puzzle out regulatory solutions for analytics. New approaches are most likely to emerge from a bottom-up discussion among different participants in diverse harmonization networks.

Finally, a revised regulation should respect subsidiarity by reducing the scope for delegated and implementing acts, which should be limited to the topics of a revised regulation, namely, those concerning field definitions and the workings of the EU Data Protection Commission. This step will leave adequate room for further policy experiments at the national level.

2. Checks and Balances. — In a revised regulation, the EU should also alter its proposed new structures to reflect the significance of checks and balances. EU law has long been attentive to checks and balances. Here too, the Lisbon Treaty is illustrative. Jean-Claude Piris, the Legal Counsel of the Council of the EU, finds the Treaty following the tradition of "successive modifications of the founding Treaties" in demonstrating a decision "not to establish any single EU institution as politically too powerful."[258] As Slaughter points out, moreover, power in the transgovernmental realm should reflect "the guarantee of continual limitation of power through competition and overlapping jurisdiction."[259] The balance of power should distribute

---

[256] *See* THOMAS H. DAVENPORT & JEANNE G. HARRIS, COMPETING ON ANALYTICS 7 (2007). For a discussion of the rise of analytics, see generally Paul M. Schwartz, *Privacy, Ethics, and Analytics*, IEEE SECURITY & PRIVACY, May/June 2011, at 66.

[257] Indeed, as Kuner notes, "the requirements for collecting and processing data in the EU will become much stricter under the Proposed Regulation." Kuner, *supra* note 173, at 224.

[258] JEAN-CLAUDE PIRIS, THE LISBON TREATY 237 (2010).

[259] SLAUGHTER, *supra* note 9, at 259.

privacy policymaking power among different EU and international institutions.

In this light, the Proposed Regulation grants the Commission a highly problematic exclusive power over the national data protection authorities. The crux of the difficulty is the Commission's veto power, which is part of the consistency process. This veto power reduces the ability of harmonization networks to develop policy and to innovate around past policy instruments now consolidated in the Proposed Regulation. It also raises important questions about the Proposed Regulation's guarantee of independence for data protection commissions. Finally, this veto power raises questions about the "democracy deficit" in the EU, which has been a longstanding matter of concern.[260]

At the same time, however, the Proposed Regulation is on the right track regarding the creation of an institution to consolidate information about different policy innovations and to prevent national regulatory efforts that are likely to impose high costs with scant privacy benefits. In their work on American federalism, Professors Malcolm Feeley and Edward Rubin note that regulatory experiments are "desirable, presumably . . . not because of an abiding national commitment to pure research but because the variations may ultimately provide information about a range of alternative governmental policies and enable the nation to choose the most desirable one."[261] Hence, whether in the United States or the EU, the need is for institutions to observe policy experiments and then adopt those with positive results and stop those with negative outcomes. These mechanisms should also be consistent with the notion of checks and balances.

Instead of recourse to the Commission, a revised regulation should create a new body, the EU Data Protection Authority. This new entity should be located within the EU Parliament, which is the sole elected branch of the EU government. The EU Data Protection Authority should consist of representatives from the Parliament; the European Data Protection Board, which is the Proposed Regulation's forum of national data protection commissioners; and the already existing European Data Protection Supervisor, an independent EU office. The EU Data Protection Authority should have the power to suspend decisions of the national authorities by a majority vote. This institution would further the establishment of checks and balances by dividing the ultimate power of the controversial new consistency process.

3. Accountability and Transparency. — For Slaughter, government officials are now becoming "enmeshed in networks of personal and in-

---

[260] For a discussion, see CRAIG & DE BÚRCA, *supra* note 146, at 133–38.

[261] MALCOLM M. FEELEY & EDWARD RUBIN, FEDERALISM: POLITICAL IDENTITY AND TRAGIC COMPROMISE 26 (2008).

stitutional relations."[262] In an age in which "[g]overnment networks pop up everywhere,"[263] the need is for government regulators to be "accountable to their national constituents" for "both domestic and international activity."[264] Regulators must be accountable to both national and global norms,[265] which is not possible if government networks do not make their activities "as visible as possible."[266] Building on this theme of accountability through transparency, Slaughter looks to judicious use of third parties to watch the governmental officials in their networked roles.[267] The EU has also been highly interested in furthering accountability and transparency. It has been leading a multipronged transparency initiative to make the Union "open to public scrutiny and accountable for its work."[268] The 2001 Laeken Declaration stressed the role of increasing the "transparency of the present institutions" as a core part of the democratic legitimacy of the EU.[269] Finally, the Lisbon Treaty has a number of articles that "insist on openness, transparency and information to the citizens."[270]

How is EU data protection policymaking to be made accountable and transparent under a revised regulation? The need here is to fulfill the aspirations of the Proposed Regulation's Article 45, which calls for collaboration in data protection on a global basis.[271] The Proposed Regulation also adopts the policies negotiated in the shadow of the Directive as well as additional global privacy policy innovations.

One way forward concerns the accountability principle. As this Article has discussed, the accountability principle, now found in the Proposed Regulation, focuses on whether a data processing entity has created internal processes that are commensurate to potential data threats. A reduction in externally imposed, formalistic bureaucratic obligations is to be offset by an organization's own risk assessments and contextual analysis. As the Article 29 Working Party acknowledges, the accountability principle leads to a "result-focused" approach.[272] One of the additional benefits of the use of accountability

---

[262] SLAUGHTER, *supra* note 9, at 7.

[263] *Id.* at 13.

[264] *Id.* at 258.

[265] *See id.* at 231–35.

[266] *Id.* at 231; *see also id.* at 235–37.

[267] *See id.* at 258–59 (proposing that the new world order "use government networks to mobilize a wide range of nongovernmental actors, either as parallel networks or as monitors and interlocutors for specific government networks").

[268] *Strategic Objectives 2005 – 2009: Europe 2010: A Partnership for European Renewal: Prosperity, Solidarity and Security*, at 5, COM (2005) 12 final (Jan. 26, 2005).

[269] The Future of the European Union, Laeken Declaration, at 23, SN 273/01 (Dec. 15, 2001).

[270] PIRIS, *supra* note 258, at 135.

[271] *See Proposed Regulation*, *supra* note 3, art. 45, at 74–75.

[272] Article 29 Data Protection Working Party, *Opinion 3/2010 on the Principle of Accountability*, at 17, 00062/10/EN, WP 173 (July 13, 2010).

mechanisms in data protection regulations should be, in turn, to make the oversight of regulators more transparent. The use of certification schemes and other measures permits oversight bodies to provide information to the regulated organizations, and to the public at large, regarding whether internal policies effectively safeguard personal information. It should also make regulatory standards more open.

Finally, there is also a need to consider accountability and transparency in the United States. The FTC is now engaged in ongoing dialogue with the EU and plays an increasingly important international role. As this Article has indicated, the FTC has found violations of the Safe Harbor by Google and Facebook and enforced this international agreement against these two companies. In the future, should EU-U.S. contacts lead to the coordination of privacy enforcement in an adjudicative fashion, there will be a need to consider the extent to which these international contacts among regulators should be made more transparent. In this regard, the Government in the Sunshine Act[273] in the United States as well as the EU's own regulations regarding transparency for governmental decisionmaking provide only incomplete models.[274] It should be noted, moreover, that there will be costs in regulatory efficiency if such international contacts occur with full public scrutiny that is carried out in real time.

IV. CONCLUSION

New conflicts in information privacy loom ahead for the United States and the EU because of the EU's Proposed Data Protection Regulation. This document, which creates directly binding law for all EU member states, alters the current equilibrium achieved under the Data Protection Directive of 1995. The Directive stimulated a process of EU-U.S. "lawmaking" through multiparty ad hoc networks and led to multiple ways of accommodating the Directive's rules for international data transfers. In contrast, the Proposed Regulation creates risks for the established processes and institutions.

In response, this Article has drawn on lessons from policymaking under the Directive. It advocates for a revised regulation that concentrates only on a limited set of nonuniform aspects of EU privacy law while also preserving future opportunities for creative global policymaking experimentation. Such a regulation should do so by focusing attention solely on the key conceptual definitions of data protection law. In addition, the revised regulation should not grant the Commis-

---

[273] Pub. L. No. 94-409, 90 Stat. 1241 (1976) (codified in scattered sections of 5 and 39 U.S.C.).

[274] *See* 5 U.S.C. § 552b(b)–(c) (2006) (noting exemptions to the kinds of meetings that must be open). For a discussion of these exemptions, see RICHARD K. BERG ET AL., AN INTERPRETATIVE GUIDE TO THE GOVERNMENT IN THE SUNSHINE ACT 65–95 (2d ed. 2005).

sion the power to act as a final arbiter of data protection standards through an ability to strike down the decisions of national data protection authorities. The revised regulation should also limit the Commission's expansive power to issue delegated and implementing acts over virtually any matter.