1999

Resolving Conflicting International Data Privacy Rules in Cyberspace

Joel R. Reidenberg
Fordham University School of Law, JREIDENBERG@law.fordham.edu

Resolving Conflicting International Data Privacy Rules in Cyberspace

Joel R. Reidenberg*

International flows of personal information on the Internet challenge the protection of data privacy and force divergent national policies and rules to confront each other. While core principles for the fair treatment of personal information are common to democracies, privacy rights vary considerably across national borders. This article explores the divergences in approach and substance of data privacy between Europe and the United States. Professor Reidenberg argues that the specific privacy rules adopted in a country have a governance function. The article shows that national differences support two distinct political choices for the roles in democratic society assigned to the state, the market and the individual: either liberal, market-based governance or socially-protective, rights-based governance. These structural divergences make international cooperation imperative for effective data protection in cyberspace. Professor Reidenberg postulates that harmonization of the specific rules for the treatment of personal information will be harmful for the political balance adopted in any country and offers, instead, a conceptual framework for coregulation of information privacy that can avoid confrontations over governance choices. The theory articulates roles for institutional players, technical codes, stakeholder summits and eventually a treaty-level "General Agreement on Information Privacy" to develop mutually acceptable implementations of the universally accepted core principles. The article concludes with a taxonomy of strategies and partners to develop international cooperation and achieve a high level of protection for personal information in international data transfers.

* Professor of Law and Director of the Graduate Program, Fordham University School of Law. A.B., Dartmouth; J.D., Columbia; D.E.A., Univ. de Paris I-Sorbonne. For provoking my early thoughts on this article at the 20th International Conference of Data Protection Authorities, I thank Juan Manuel Fernandez Lopez, Director of the Spanish Data Protection Agency. For their discussion and insights on earlier portions and drafts of this article, I thank Anne Carblanc, Richard Carnell, Julie Cohen, Jill Fisch, Robert Gellman, Robert Kaczorowski, Mark Patterson, Russell Pearce, Charles Raab, Paul Schwartz, and Steve Thel. Work on this paper was supported in part by a Fordham Law School Faculty Summer Research Grant Award and benefited from my colleagues' discussion at the Fordham Faculty Workshop. All opinions, errors, omissions, and misunderstandings remain my own. All Internet citations were current as of May 22, 2000.

INTRODUCTION

The robust development of the Internet and online services over the last several years represent the most significant era for international flows of personal information since the first wave of computerization in the 1970s. During the early days of data processing, fears of omnipotent and omnipresent collections of personal information were largely conceived in terms of centralized computing and foreign data havens akin to tax havens.[1] Until the

1. *See, e.g.*, ANDRÉ LUCAS, LE DROIT DE L'INFORMATIQUE 67 (1987) (describing the fear of data havens); PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) (expressing concern about intrusions into personal privacy by government and

personal computer revolution, large scale processing of personal information was generally reserved to institutions with centralized databases.[2] The Internet and personal computers, however, multiply the number of participants generating and using personal information in a way that was unimaginable a generation ago. Every personal computer, Internet service provider, and Web site can now create, collect, and process personal information. Although cross-border transfers of data have been occurring for many years, the growth trends in Internet data transfers reflect both a quantitative and qualitative shift.[3]

In particular, the dramatic growth of Internet services during the last several years and the decentralization of information processing arrangements have exponentially increased the flow of personal information across national borders. From the processing of German railway card data in the United States[4] to the sale of French gastronomic products through the Hong Kong Web site of Marché de France,[5] personal data is driving the global economy and fair information practices have never been more important for the protection of citizens. In the United States, the sale of personal information alone was estimated at $1.5 billion in 1997[6] and confidence in the fair treatment of personal information is at a critical juncture.[7] Governments around the world have unequivocally declared that the future protection of

large corporations); Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1107-27 (1969) (identifying concerns regarding centralized processing of information about individuals).

2. *See, e.g.*, Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 99-103 (Philip E. Agre & Marc Rotenberg eds., 1997) (noting that the development of global networks has exacerbated privacy concerns); Viktor Mayer-Schonberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 225 (Philip E. Agre & Marc Rotenberg eds., 1997) (noting that "minicomputers" allowed small organizations to use decentralized data processing).

3. *See* Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 557-61 (1998) (arguing that the Internet creates a quantitative and qualitative change in privacy).

4. *See* Alexander Dix, *The German Railway Card: A Model Contractual Solution of the "Adequate Level of Protection" Issue?*, PROC. XVIII INT'L CONF. DATA PROT. COMM'RS (1996) <http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex3.htm> (describing a data protection agreement between the German railway and Citibank).

5. *See Le Marché de France* <http://195.114.67.153/cgi-bin/ncommerce/ExecMacro/lemarche>; *see also* Serge Gauthronet & Frédéric Nathan, *On-line Services and Data Protection and the Protection of Privacy* 50-51 (1998) [hereinafter *On-line Services*] <http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf> (explaining the international architecture of the company's Web site).

6. *See* Trans Union Corp., F.T.C. No. 9255 ¶ 354 (July 31, 1998) <http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf> (estimating the sale of personal information in 1997).

7. *See* Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 106 (1995) (discussing the transformative impact of new information technology on economic, political, and social organization).

citizen privacy is essential to the robust development of electronic commerce.[8]

At the same time, however, privacy rights for personal information vary considerably across national borders.[9] The United States, for example, has a market-dominated policy for the protection of personal information and only accords limited statutory and common law rights to information privacy.[10] In contrast, European norms reflect a rights-dominated approach and the European Union now requires each of its Member States to have comprehensive statutory protections for citizens.[11] International data flows on the Internet, whether for execution of transactions or intracorporate data management, force these divergent data protection policies and rules to confront each other with ever greater frequency.[12] Indeed, the Internet and electronic commerce

---

8. *See generally OECD Ministerial Conference Conclusions: "A Borderless World: Realising the Potential of Global Electronic Commerce,"* ORG. EC. COOPERATION DEV. (OECD) DOC. SG/EC(98)14/FINAL Ann. III (1998) <http://www.olis.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/88e869fb73a5a5e0c12566de004ec962/$FILE/12E81007.ENG> [hereinafter *A Borderless World*] (noting determination of OECD to work with international agreements and businesses to protect data privacy); *A European Initiative in Electronic Commerce: Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions* <http://www.ispo.cec.be/Ecommerce/legal/documents/com97-157/ecomcom.pdf> [hereinafter *European Initiative in Electronic Commerce*] (noting the need to protect personal data privacy to help advance electronic commerce in Europe); THE WHITE HOUSE, *A Framework for Global Electronic Commerce* (July 1, 1997) <http://www.ecommerce.gov/framewrk.htm> (discussing e-commerce development and privacy in the United States).

9. I will use the terms "data privacy," "information privacy," "data protection," and "fair information practices" interchangeably. For a discussion of privacy terminology, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 5-6 (1996).

10. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 101-32 (1997) (noting that the U.S. government should play a limited role in protecting data but should articulate broad principles to guide industry); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN DATA PROTECTION DIRECTIVE 2-3 (1998) (arguing that there is a potential for significant economic conflict between Europe and the United States if the gulf in data privacy protection is not bridged). *See generally* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992) (comparing the American self-regulation model with the more ambitious state-sponsored protections provided in Sweden, West Germany, and Britain); SCHWARTZ & REIDENBERG, *supra* note 9 (comparing relative levels of data protection provided in the United States and Europe).

11. *See generally 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 Free Movement of Such Data*, 1995 O.J.(L 281) 31 <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html [hereinafter *European Data Protection Directive*] (setting out the standards for implementation in each of the 15 Member States of the European Union).

12. *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995) (noting the significant challenges to the flow of data between the United States and Europe in the context of European data protection laws and the "data embargo order").

raise the stakes for individuals, businesses and government. In the absence of coherent privacy protection, data flow embargoes are increasingly likely.[13]

Part I of this article defines characteristics of information flows on the Internet that challenge the protection of information privacy and set the stage for serious confrontation between different national and transnational data protection standards. Part II identifies a core set of principles for fair information practice that is common to strong democracies. While an international consensus exists on the basic standards for the fair treatment of personal information, significant differences in both approach and substance persist, particularly between Europe and the United States.[14] Part III shows that the characteristics of information flows and these differences result in serious conflict between normative data protection objectives around the world.[15]

Part IV of the article argues that the specific privacy rules in any particular country have a governance function reflecting the country's choices regarding the roles of the state, market, and individual in the country's democratic structure. Under this governance theory of privacy, national differences derive from distinct visions of governance, and privacy rules strive to protect a state's norm of governance, whether it be a liberal market norm

13. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 380-81 (noting that national laws in most European Union Member States permitted blocking data transfers if the destination has insufficient privacy standards and the European Data Protection Directive requires blocking).

14. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973) [hereinafter H.E.W. GUIDELINES] (advising a complete set of rights of citizens with respect to the computerized processing of their personal information); *Consumer Privacy on the World Wide Web: Hearings Before the Subcomm. on Telecomm., Trade and Consumer Protection of the House Comm. on Commerce*, 105th Cong. (July 21, 1998) <http://www.ftc.gov/os/1998/9807/privac98.htm> (prepared statement of Robert Pitofsky, Chairman of the FTC) (describing the FTC's position on the privacy protections necessary for American citizens); *European Data Protection Directive*, *supra* note 11 (setting out privacy standards for the 15 Member States of the European Union); Council of Europe (COE), Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 20 I.L.M. 377 (1981) [hereinafter COE Convention] (defining the standards for adoption by signatory countries to the international treaty); OECD, Guidelines on Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, 20 I.L.M. 422 (1981) <http://coe.fr.eng/leglatxt/108e.htm> [hereinafter OECD Guidelines] (recommending a set of standards for adoption in member countries). *See generally* BENNETT, *supra* note 10 (explaining different solutions to privacy protection in different countries); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989) (critiquing the differences in government data protection); SCHWARTZ & REIDENBERG, *supra* note 9 (comparing U.S. law and practice to European standards and finding important differences); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967) (describing perspectives on privacy from different cultures).

15. *See generally* SCHWARTZ & REIDENBERG, *supra* note 9 (analyzing the differences between the U.S. and European approaches and standards); SWIRE & LITAN, *supra* note 10 (arguing for confrontational differences between the United States and Europe); Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137, S148-60 (1992) (describing differences between ad hoc and omnibus approaches).

or a socially-protective, citizen's rights norm. This insight means that efforts to harmonize specific standards would conflict with the way any given model embodies a market-based or a rights-based philosophy of governance.

If the harmonization of privacy rules is, thus, harmful for the political balance adopted in any country, then the peaceful coexistence of different privacy rules becomes essential to avoid online confrontations. Part V presents a theory for the coregulation of information privacy that identifies key institutional players and mechanisms to minimize regulatory conflict. And finally, Part VI offers short- and long-term strategies for coordination and cooperation among different privacy regimes. The article concludes with a discussion of the effect that this coregulation might have on the governance norms that posed the original conflicts.

I. DATA FLOW CHARACTERISTICS

On the Internet, four characteristics frame the international transfer of personal information. These characteristics reflect a trend that marks dramatically increased capacity and incentives to abuse personal information across national borders. The salient points range from the actual uses of deployed technologies (specifically, collecting clickstream information and multinational processing) to the commercial incentives that drive the processing of personal information (notably, data warehousing and profiling). Taken together, these characteristics set the stage for intense conflicts over information privacy.

A. *Clickstream Data*

In a network environment, every click of a computer's mouse leaves a data trace.[16] This "clickstream data" is far more robust than the typical "transaction data" from an electronic payment or telephone call. "Transaction data" typically contain discrete information on the parties, date, time and type of transaction.[17] In contrast, by its very nature, the clickstream reflects

16. For useful illustrations, examine the cookies.txt files, the .hst files or the cache subdirectory files on any personal computer. The cookies.txt files contain information about actions taken by a user at specific websites. *See Persistent Client State HTTP Cookies* <http://home.netscape.com/newsref/std/cookie_spec.html> (describing information that can be stored on a client's hard drive when he connects to a server). The .hst files contain the addresses of all recently visited websites accessed by the personal computer and the cache subdirectory contains copies of the Web pages and images recently viewed on the personal computer. Often, similar data reflecting a user's activities will be hidden on the hard drive. *See* Peter H. Lewis, *What's on Your Hard Drive?*, N.Y. TIMES, Oct. 8, 1998, at G1 (noting that people may be unaware that sensitive and embarassing files may be found on their computers).

17. *See, e.g.*, Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115, FCC

not just the existence of interactions, but also includes the content of those interactions; every keystroke is included in the clickstream and not just the fact that an interaction took place. The clickstream information provides continuous, recordable surveillance of individuals and all of their activities.

This clickstream information is increasingly sought. For example, software is now readily available and used to establish monitoring programs for clickstream data in the workplace.[18] As the Internet economy moves society from an economy of mass production to mass customization, transaction-generated information becomes an integral part of the process to predict and modify consumer behavior.[19] On the Internet, most websites collect some clickstream data in the form of log files.[20] These log files routinely collect the Internet addresses of visitors browsing the site and record the Web pages that the visitors read.[21] Internet service providers similarly can record logs of all subscribers' interactions, but, for the moment, are unlikely to retain the clickstream information. The sheer volume of such records exceeds the usefulness for Internet service providers. Nevertheless, advertising arrangements on the Internet seek to recapture the attributes of the clickstream data that the online service providers forgo. Companies such as DoubleClick[22]

98-27 (rel. Feb. 26, 1998) <http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt>; NATIONAL TELECOMM. AND INFO. ADMIN. (NTIA), U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995) <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html> (describing the ease with which transaction data can be accessed by private individuals).

18. For example, a product called Surf Control Scout is designed to show employers "'who's doing what and when.'" Surf Control Scout Corp., *Internet Monitoring and Reporting* <http://www.surfcontrol.com/products/index.html>. There is even a monitoring product offered to network administrators that is called "Little Brother." *See* Kansmen Corp., *Kansmen Corporation Announces LittleBrother 2.0*, Oct. 22, 1997 <http://www.littlebrother.com/products/lb/pr.htm>. Nearly two-thirds of U.S. employers report that they implement employee surveillance programs. *See* AMERICAN MGMT. ASS'N INT'L, 1997 AMA SURVEY: ELECTRONIC MONITORING & SURVEILLANCE 1 (1997) <http://www.amanet.org/survey/elec97.htm>.

19. *See* Rohan Samarajiva, *Interactivity as though Privacy Mattered*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 21, at 277-81 (discussing the trend toward mass customization and the threat it poses to personal privacy).

20. *See* Joseph I. Rosenbaum, *Privacy on the Internet: Whose Information Is it Anyway?*, 38 JURIMETRICS J. 565, 571-572 (1998) (discussing how the Internet contributes to the "dossier effect" in which large amounts of small pieces of information about individuals are amassed). *See generally* Jean-Marc Dinant, *Les traitements invisibles sur Internet* (June 1998) <http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html> (describing hidden collections of personal information on the Internet).

21. Network operating software can be configured to record the log files as a default. System operators must affirmatively disable the feature. *See* Cliff Wootton, *Analyzing Log Files*, WEB DEVELOPER'S J. <http://www.webdevelopersjournal.com/articles/log_analysis.html>.

22. DoubeClick's Web site is located at <http://www.doubleclick.com>.

propose through the use of "cookies" technology to track Internet users' browsing patterns across many websites.[23]

In effect, clickstream data offer a quantitative leap forward in the amount of personal information in circulation.[24] At the same time, the surveillance aspect of clickstream data is also qualitatively different from earlier forms of transaction data. The detail offers a picture that was previously not readily compiled. While the depth of information available from clickstream data might have been obtainable with a private investigator recording an individual's every move, such surveillance would have been treated as harassment. In the past, privacy was preserved from the isolation of discrete bits of information. The difficulty in assembling such information provided protection to individuals.[25] Clickstream data break down this protection.

B. *Multinational Sourcing*

The Internet and emerging electronic commerce activities encourage multinational sourcing of information.[26] The entire architecture of the Internet is based on the principle of geographic indeterminacy. The information processing capabilities of the network were designed to make distance and geographic location irrelevant. As a result, servers and processing arrangements migrate; data may be stored in one location and readily shifted to another location just as transmission and computing resources may be moved instantaneously from one place to another.[27] Corporate intranets, built using some of the same technology as the Internet, have adopted the same features.[28] Data may be collected in one location, processed elsewhere, and

---

23. *See DoubleClick Privacy Statement* <http://www.doubleclick.com/privacy_policy/> (describing the company's policy regarding information collection and use); *On-line Services*, *supra* note 5, at 80-95 (discussing DoubleClick's development, operation, and data protection practices).

24. *See* Schauer, *supra* note 3, at 557-59 (discussing the quantitative increase in data availability).

25. *See id.* at 559 (noting that modern information technology allows access to information previously unavailable).

26. *See, e.g.*, OECD, THE ECONOMIC AND SOCIAL IMPACTS OF ELECTRONIC COMMERCE: PRELIMINARY FINDINGS AND RESEARCH AGENDA Chap. 3 (1999) <http://www.oecd.org/subject/e_commerce/summary.htm> [hereinafter IMPACTS OF ELECTRONIC COMMERCE]; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, *in* GOBALISATION AND THE INFORMATION SOCIETY: THE NEED FOR STRENGTHENED INTERNATIONAL COORDINATION COM(98)50 § 2.1 <http://europa.eu.int/comm/dg03/publicat/comms/infosoc/comiscen.pdf> (discussing the growth of global electronic commerce).

27. *See* CATE *supra* note 10, at 10 (discussing the original ARPANET and how it "encouraged the creation of multiple links among the computers on the network"); IMPACTS OF ELECTRONIC COMMERCE, *supra* note 26, at 79 (discussing technology diffusion and interfirm collaboration as changes brought about by the growth of electronic commerce).

28. *See generally* Deborah Asbrand, *Banking on Intranet Training: Citibank's Net Division Delivers Soft Skills and Technology with Online Training Courses*, INTRANET J., Aug. 23, 1999

stored at yet another site. In addition, the open architecture also means that multiple intermediaries have access to and may process data in transit.[29] For example, third-party data collectors, such as Internet advertising companies like DoubleClick, obtain and pass on information about other websites' visitors. These arrangements radically increase the complexity of data processing and obscure the responsibility for data protection.

C. *Data Warehousing and Data Creep*

With the costs of computing and storage diminishing rapidly, isolated bits of data that in the past were useless or too expensive to process may now be collected and retained.[30] Since information will always have value in an "Information Society," the almost zero cost of processing incremental bits of data offers a powerful incentive for "data warehousing." "Data warehousing" is the stockpiling of millions of bits of personal information for future analysis. While each isolated piece of information may have little meaning or risk minimal potential harm to the individual, the aggregate collection takes on an entirely different character. Analyzing the aggregate can reveal patterns of behavior, profiles, and an intimate slice of the lives of individuals, which can be used to categorize and segregate individuals in society.[31]

"Data creep" is closely related to data warehousing. "Data creep" represents the "more is better" school of thought.[32] More and more bits of personal information are sought because of a vague belief that somehow the

---

<http://www.intranetjournal.com/deployment/web_training_082399.html> (describing Citibank's use of Web technology for intranet development).

29. *See* IMPACTS OF ELECTRONIC COMMERCE, *supra* note 26, at 79-103 (addressing the changing business models and market structures).

30. *See, e.g.*, CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 33-34, 36-37 (1999) (discussing the collection of consumer information); PRIVACY WORKING GROUP, U.S. DEP'T OF COMMERCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION ¶ 6 (1995) <http://www.ittf.nist.gov/documents/committee/infopol/niiprivprin_final.html> ("[B]ecause the costs associated with storing, processing, and distributing personal records are continuously decreasing, accumulating personal information from disparate sources will become a cost-effective enterprise for information users with interests ranging from law enforcement to direct marketing.").

31. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1239-41 (1998) (discussing the construction and economic value of detailed personal profiles to database marketing firms).

32. "Data creep" is analogous to "function creep." In political science terms, "function creep" describes the tendencies of bureaucracies to gradually expand their functions or missions. "Data creep" is the tendency to continually expand the scope of collection and use of personal information. *See, e.g.*, Samarajiva, *supra* note 19, at 301 (noting the "'creeping' redesign of public telecommunication networks throughout the world to include covert surveillance capabilities").

information will have use.[33] Since the cost to collect and process information has dropped and the push for data warehousing has grown, more seemingly innocuous information is collected from individuals for storage and future processing. For example, companies now ask for a customer's zip code even if the purchase transaction is conducted with cash.[34] A company does not need the customer's zip code to process cash transactions. But, the zip code offers a key piece of data to generate demographic profiles. By aggregating innocuous information or seemingly anonymous data, the construction of detailed individual profiles becomes routine.

D. *Pressures for Secondary Use and Profiling*

The ease of collecting and storing personal information coupled with an enhanced capability to use it create tremendous commercial pressures in favor of unanticipated or secondary uses.[35] U.S. industry has a long and entrenched tradition of surreptitious and secondary use of personal information.[36] These diverted uses of collected personal information can generate additional value. In the name of efficiency, an existing pool of personal information becomes an attractive source of data for new uses.[37] This diversion of personal information is particularly acute with respect to profiling. Something as routine as a magazine subscription becomes the basis for a detailed profile of interests. Once a substantial database exists, the ability to profile individuals within the database becomes easier and more valuable.[38]

---

33. *See* Kang, *supra* note 31, at 1239 ("A sophisticated database marketing initiative thus acquires as much data on potential customers as legally possible.").

34. Staples, the office supply store chain, routinely asks customers for their zip code. The cashiers at Office Max, a competing chain, cannot process credit card transactions without storing a digital image of the customer's signature unless the manager intervenes.

35. *See* Adam L. Penenberg, *On the Web, No One Is Anonymous*, FORBES, Nov. 29, 1999, at 184-85 http://www.forbes.com/forbes/99/1129/6413182s1.htm (noting the existence of a Microsoft "watermark" and other technology that allows websites to track users).

36. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 391-92 (discussing the greater tolerance for secondary use of personal information in the United States versus Europe); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 530 (1995) [hereinafter Reidenberg, *Setting Standards*] ("As seen in the direct marketing and employment contexts, secondary use is a problem in the U.S. private sector, particularly with respect to marketing applications.").

37. *See* H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 7-8 (1994) (discussing the concern that privacy is harder to maintain with increasing computerization).

38. *See, e.g.*, Kang, *supra* note 31, at 1238-41 (discussing the myriad opportunities for "data mining" once large databases have been constructed); Josh Mchugh, *Mind Readers*, FORBES, Nov. 29, 1999, at 188-89 http://www.forbes.com/forbes/99/1129/6413182s4.htm (noting the "wealth of data" Yahoo! Gathers on its customers).

II. INTERNATIONAL DATA PRIVACY PRINCIPLES

These information processing characteristics present the same problem for citizens around the globe; namely, how to assure privacy in the complex world of online transactions. Norms for the treatment of personal information exist and share many common attributes across different legal systems and cultures.[39] As illustrated in multilateral instruments[40] and academic scholarship,[41] democracies converge on a basic set of principles for "data protection" or "data privacy." These norms of fair information practice constitute what can be termed First Principles, and their acceptance separates democratic societies from totalitarian regimes.[42] Yet, important divergences in the execution of these First Principles can be found at the national level.[43] For the Internet, these divergences promote significant conflict.

A. *Convergence on First Principles*

In democracies around the world, information privacy is recognized as a critical element of civil society[44] and as a necessity for the development of the Internet.[45] Trust and confidence online will not be possible without data

39. *See, e.g.*, WESTIN, *supra* note 14, at 29-30 (illustrating that concern for privacy protection is a cross-cultural phenomenon).

40. *See, e.g.*, COE Convention, *supra* note 14; OECD Guidelines, *supra* note 14; *European Data Protection Directive*, *supra* note 11.

41. For a scholarly discussion of data privacy in a democracy see generally BENNETT, *supra* note 10, at 96-111; CATE, *supra* note 10; FLAHERTY, *supra* note 14; WESTIN, *supra* note 14; Bennett, *supra* note 2; Robert Gellman, *Conflict and Overlap in Privacy Regulation: National, International, and Private*, *in* BORDERS IN CYBERSPACE: INTERNATIONAL POLICY AND THE GLOBAL INFORMATION INFRASTRUCTURE 255 (Brian Kahin & Charles Nesson eds., 1997).

42. Data protection is necessary to protect citizen freedoms and liberties from totalitarian repression. *See* Charles D. Raab, *Privacy, Democracy, Information*, *in* THE GOVERNANCE OF CYBERSPACE 161 (Brian D. Loader ed., 1997); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987) (discussing the West German Federal Constitutional Court's protection of information collected in the census as a way to protect other constitutional rights).

43. *See, e.g.*, BENNETT, *supra* note 10, at 193-219 (explaining the differences in data protection practices between Sweden, West Germany, Britain, and the United States); JOEL R. REIDENBERG & PAUL M. SCHWARTZ, ON-LINE SERVICES AND DATA PROTECTION AND PRIVACY: REGULATORY RESPONSES (1998).

44. *See* Michael Donald Kirby, *Privacy Protection-A New Beginning?*, *in* PROC. XXI INT'L CONF. DATA PROT. COMM'RS (1999) <http://www.pco.org.hk/conproceed.html> [hereinafter PROC. XXI INT'L CONF.] (arguing that "[w]hat is at stake [with privacy] is nothing less than the future of the human condition"); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 557 (1995) (arguing that a goal of data protection is to protect deliberative democracy).

45. *See* A Framework for Global Electronic Commerce, *supra* note 8, at 13-14 (pledging U.S. support for personal data privacy protection to ensure continued growth of the Internet).

protection.[46] The most common definition of information privacy is the right of the individual to "information self-determination."[47]

Over the last thirty years, governments and theorists around the world have identified a core set of fair information practices to assure citizens' participation in the collection and use of their personal information. These benchmarks form the First Principles of information privacy and revolve around four sets of standards: (1) data quality; (2) transparency or openness of processing; (3) treatment of particularly sensitive data, often defined as data about health, race, religious beliefs, and sexual life among other attributes; and (4) enforcement mechanisms.[48] In examining the emergence of national data privacy rules, Professor Colin Bennett has shown a high degree of policy convergence regarding the treatment of personal information.[49] Professor Bennett distills these standards into ten elements that parallel the 1972 recommendation of the Younger Committee in the United Kingdom,[50] namely that an organization:

- Must be *accountable* for all personal information in its possession;
- Should *identify the purposes* for which the information is processed at or before the time of collection;
- Should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);
- Should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;

---

46. *See* European Initiative in Electronic Commerce, *supra* note 8, at 20 (discussing the need to create consumer confidence). *See generally* FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: REPORT TO CONGRESS (1999) <http://www.ftc.gov/opa/1999/9907/report1999.htm> [hereinafter SELF-REGULATION]; FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998) <http://www.ftc.gov/reports/privacy3/toc.htm> [hereinafter PRIVACY ONLINE] (discussing the FTC's approach to online privacy).

47. The term "information self-determination" was first used in a famous German census decision. *See Census Act of 1983 Partially Unconstitutional*, Judgment of the First Senate (Karlsruhe, Dec. 15, 1983), *translated in* 5 HUM. RTS. L.J. 94 (1984); Simitis, *supra* note 42, at 734-35 (discussing the ruling in the German census case). The American formulation, according the individual control over the disclosure of personal information, traces its roots to a study project of the Association of the Bar of the City of New York, later published by Alan Westin. *See* WESTIN, *supra* note 14, at xiii. Attributed to Alan Westin, rather than the Bar project, this formulation defines information privacy as the right of the individual to control the use of personal information: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." *Id.* at 7. More recently, Paul Schwartz has argued that the "control" definition of privacy misses important contextual distinctions in modern society. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1663-65 (1999).

48. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 12-17 (discussing the development and substance of the First Principles in Europe); Reidenberg, *Setting Standards*, *supra* note 36, at 512-16.

49. *See* BENNETT, *supra* note 10, at 95-115.

50. In May 1970, the British Labour government appointed an interdepartmental committee to study privacy issues and report back to Parliament. *See id.* at 85-86. The chair of the committee was Sir Kenneth Younger. *See id.* at 85.

- Should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality principle*);
- Should *retain* information only as long as necessary;
- Should ensure that personal information is kept *accurate, complete, and up to date*;
- Should protect personal information with appropriate *security safeguards*;
- Should be *open* about its policies and practices and maintain no secret information systems;
- Should allow data subjects *access* to their personal information, with an ability to amend it if necessary.[51]

In the context of the Internet, these First Principles remain as important as ever. As the Internet increases the capacity and incentive for organizations to engage in information trafficking, rigorous application of the First Principles becomes ever more critical. In particular, information flows on the Internet might readily infringe the norms that require: (1) the specification of the purpose for data collection; (2) the consent of individuals in connection with the treatment of their personal information; (3) the transparency of data practices for individuals, including awareness of data collection and access to stored personal information; (4) special protection for sensitive data; and (5) the establishment of enforcement remedies and mechanisms.

Nevertheless, the wide degree of international consensus on the First Principles is reflected in major policy instruments and national laws that, over the years, endorsed the norms.[52] The United States, for example, has through law adopted various data privacy standards and relied on self-restraint to fill the gaps in protection.[53] Although the resulting standards hardly address the full set of First Principles (in particular with respect to transparency of processing and secondary use of personal information)[54] the

---

51. Colin J. Bennett & Rebecca Grant, *Introduction*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 6 (Colin J. Bennett & Rebecca Grant eds., 1999) [hereinafter VISIONS OF PRIVACY].

52. *See generally* THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS (Marc Rotenberg ed., 1999) (consolidating the texts of various national laws and international instruments on data privacy).

53. *See* Privacy Act of 1974, 5 U.S.C. § 552a (1994) (regulating government data processing); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (1994) (regulating credit reporting); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2501 (1994) (providing for privacy of electronic communications); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994) (regulating privacy for video rental customers); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994) (protecting privacy of cable subscribers). *See generally* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993) (discussing the attempts and failures to enact statutory protections incorporating the full set of First Principles).

54. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 379-405 (showing that law and practice in the United States fail to respond to the complete set of norms, but do include narrow protections that cover some of the elements of the First Principles).

United States has made a public commitment to the broader set of First Principles. Beginning in 1973, the U.S. Department of Health, Education, and Welfare elaborated one of the first full codes of fair information practice.[55] The code embodied norms for transparency of data processing, access to stored personal information, restrictions on secondary use of personal information, correction of erroneous information, accuracy, and security safeguards.[56] Fifteen years later, the Clinton Administration recognized that the complete set of First Principles were still the basis for privacy protections. But despite the failure of non-regulatory policies to succeed in protecting information privacy, the Administration still sought industry development of voluntary codes.[57]

During the 1970s and 1980s, national laws in Europe emerged that contained comprehensive standards embodying the First Principles.[58] By the early 1980s, international instruments ratified this basic common set of principles for data protection. The Organization for Economic Cooperation and Development (OECD), comprised of the major industrialized nations of the world, adopted voluntary guidelines for fair treatment of personal information.[59] Justice Michael Kirby of Australia, the chairman of the OECD group drafting the voluntary guidelines observed: "Surprisingly, in all of the major international efforts that have so far addressed . . . [data protection], there has been a broad measure of agreement on the 'basic rules' around which domestic privacy legislation should cluster."[60] Contemporaneously, the Council of Europe, a post-World War II intergovernmental organization dedicated to the protection of human rights, opened for signature an international treaty adopting essentially the same norms for data privacy, but the treaty created binding rules for signatories.[61] These instruments provided a model for later international laws such as the New Zealand data protection act.[62] By 1990,

55. *See* H.E.W. GUIDELINES, *supra* note 14.

56. *See id.*

57. *See generally* U.S. DEP'T OF COMMERCE, PRIVACY AND ELECTRONIC COMMERCE (1998) <http://www.doc.gov/ecommerce/privacy.htm> (showing that the OECD Guidelines containing the complete set of First Principles is the guidepost for privacy protection and calling on industry to develop private sector codes of conduct); PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE, *supra* note 30 (rephrasing First Principles in the context of the Clinton Administration's Internet policy). For a highly critical view of U.S. policy, see generally Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999).

58. For a description of statutory developments in the area of data privacy, see generally FLAHERTY, *supra* note 14; BENNETT, *supra* note 10, at 95-115.

59. *See* OECD Guidelines, *supra* note 14.

60. Michael D. Kirby, *Transborder Data Flows and the "Basic Rules" of Data Privacy*, 16 STAN. J. INT'L L. 27, 29 (1980).

61. *See* COE Convention, *supra* note 14. The convention, however, requires safeguards for sensitive data unlike the OECD guidelines which are silent on the issue. *See id.*

62. *See, e.g.*, Blair Stewart, Adequacy of Data Protection Measures: The New Zealand Case, Paper presented at the 12th Privacy Laws & Business International Conference, Cambridge, U.K., June 29, 1999 <http://www.privacy.org.nz/media/adequacy.html> (noting that New Zealand's law

even the United Nations had adopted a resolution affirming the First Principles as a global imperative.[63]

More recently, in 1995, the European Union concluded a regulatory process that culminated in the adoption of the European Directive on Data Protection.[64] The Directive requires that the Member States of the European Union enact national legislation conforming to a defined set of substantive standards.[65] Europe's goal is to harmonize fair information practices at a high level of protection. This set of standards is a comprehensive endorsement of First Principles, and has become the model for legislation in many non-European countries.[66]

As a further demonstration of this consensus on First Principles, today in Eastern Europe and in South America, data protection has become a critical part of the national movements to establish open, democratic societies.[67] Indeed, the international community has affirmed the applicability of First Principles to Internet activities.[68]

---

was modeled on the OECD Guidelines); HUNGARIAN REPUBLIC, THE FIRST THREE YEARS OF THE PARLIAMENTARY COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION 66 (1998) [hereinafter HUNGARIAN REPORT] (reporting that the Council of Europe Convention was the model for Hungarian data protection).

63. *See Guidelines for the Regulation of Computerized Personal Data Files*, U.N. GA Res. 45/95 (1990) <http://www.unhchr.ch/html/menu3/b/71.htm> (adopting "Guidelines for the Regulation of Computerized Personal Data Files").

64. *See European Data Protection Directive*, *supra* note 11. For a discussion of the adoption process, see Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV 445 (1995).

65. For a discussion of the European law-making process see GEORGE A. BERMANN, ROGER J. GOEBEL, WILLIAM J. DAVEY & ELEANOR M. FOX, CASES AND MATERIALS ON EUROPEAN COMMUNITY LAW (1993 & Supp. 1995).

66. Many Eastern European countries, including Hungary, the Czech Republic, and Slovenia, along with Latin American countries such as Chile and Argentina, have adopted or are in the process of adopting European-style laws. *See* CATE, *supra* note 10, at 45-47 (1997) (discussing the European consensus on privacy principles); HUNGARIAN REPORT, *supra* note 62, at 68 & n.19 (indicating the use of the European Data Protection Directive to promote development of Hungarian law).

67. *See* HUNGARIAN REPORT, *supra* note 62, at 11; Pablo A. Palazzi, *Proteccion de Datos, Privacidad y Habeas Data en America* <http://members.theglobe.com/pablop/LatinoAmerica.html ?nfhp=948126670&rld=446232546> (compiling data protection laws and jurisprudence in Latin America). Even in Asia, global trade and services along with the recognition and expectation of the affluent countries for the respect of human rights has led to interest in the First Principles. *See* Stephen Lau, *The Asian Status with Respect to the Observance of the OECD Guidelines and the EU Directive*, *in* PROC. XIX INT'L CONF. DATA PROT. COMM'RS (1997) <http://www.privacy.fgov.be/conference/authors.html> [hereinafter PROC. XIXTH INT'L CONF.].

68. *See, e.g.*, *Ministerial Declaration on the Protection of Privacy on Global Networks*, OECD Doc. DSTI/ICCP/REG(98)10, FINAL (Dec. 18, 1998) <http://appli1.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/61c1c8c0a31f9457c12566de00506c13/$FILE/12E81013.ENG> [hereinafter *Ministerial Declaration*] (reaffirming the 1980 OECD Guidelines for global networks); Working Party Established under Art. 29 of Directive 95/46/EC, *Working Document: Processing of Personal Data on the Internet*, E.C. Doc. DG XV 5013/99 WP 16 (Feb. 23, 1999) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp16en.htm> [here-

B. *Divergence on Execution*

Even though democracies have converged on First Principles and have reaffirmed their applicability to the Internet, studies of national legislation and data protection policies in numerous countries reflect varying degrees of adherence to these basic principles.[69] In effect, the execution of First Principles diverges significantly across countries. At the outset, national policies can implement First Principles in multiple ways; some effective, others not. More subtly, national policies may interpret First Principles quite differently. These divergences in execution present a fundamental challenge to Internet information flows and the structure of information-processing activities on the global network. The danger is that seemingly small differences can have significant effects as obstacles to online services or as incentives for the distortion of services.[70]

1. *Implementation.*

There are three approaches to the implementation of First Principles. The predominant approach, found outside the United States, is a comprehensive data protection law. Under this model, omnibus legislation strives to create a complete set of rights and responsibilities for the processing of personal information, whether by the public or private sector.[71] First Principles become statutory rights and these statutes create data protection supervisory agencies to assure oversight and enforcement of those rights.[72] Within this framework, additional precision and flexibility may also be achieved through codes of conduct and other devices.[73] Overall, this implementation approach treats data privacy as a political right anchored among the panoply of funda-

---

inafter *Processing of Personal Data*]; Recommendation No. R(99)5 of the Comm. of Ministers, Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways (Feb. 23, 1999) <http://www.coe.fr/DataProtection/elignes.htm>.

69. *See, e.g.*, Sophie Louveaux, Comment concilier le commerce electronique et la protection de la vie privée?, *in* Etienne Montero ed., DROIT DES TECHNOLOGIES DE L'INFORMATION: REGARDS PROSPECTIFS (Etienne Montero ed. 1999); REIDENBERG & SCHWARTZ, *supra* note 43; SCHWARTZ & REIDENBERG, *supra* note 9; ADRIANA C.M. NUGTER, TRANSBORDER FLOW OF PERSONAL DATA WITHIN THE EC (1990).

70. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 142-49.

71. *See* CATE, *supra* note 10, at 32-48 (describing the content of data privacy laws of European countries and multinational organizations).

72. *See* BENNETT, *supra* note 10, at 153-92 (explaining how the First Principles were implemented in Sweden, West Germany, Britain, and the United States).

73. *See* Stefano Rodota, *Internet: Electronic mail, electronic sales, ethical codes*, *in* PROC. XX INT'L CONF. DATA PROT. COMM'RS (1998).

mental human rights and the rights are attributed to "data subjects" or citizens.[74]

In the second approach to implementation, found in the United States, the role of the state is far more limited. Legal rules are relegated to narrowly targeted sectoral protections. For example, the Video Privacy Protection Act prohibits the disclosure of titles of particular films rented by a customer at a video store,[75] while viewing habits on the Internet of streaming video remain unprotected. Under this sectoral approach, the primary source for the terms and conditions of information privacy is self-regulation. Instead of relying on governmental regulation, this approach seeks to protect privacy through practices developed by industry norms, codes of conduct, and contracts rather than statutory legal rights. Data privacy becomes a market issue rather than a basic political question, and the rhetoric casts the debate in terms of "consumers" and users rather than "citizens."[76]

The third approach to implementation of First Principles is technical. Under this "code" or "lex informatica" model,[77] engineering specifications embody policy rules for data protection. This is particularly noteworthy for privacy rules in the online environment. Technical rules and default settings establish data privacy norms.[78] This approach is, thus, a hybrid: The model contains formal rules but is neither state regulation nor industry self-regulation. Unlike state-centric policymaking in the case of comprehensive statutes and industry-centric policymaking in the case of self-regulation and

---

74. *See generally* notes 184-215 *infra* and accompanying text; CATE, *supra* note 10, at 42-43 (discussing the importance of privacy in the European Directive; Simitis, *supra* note 64 (discussing the E.U. Member States' emphasis on protecting personal privacy rights).

75. *See* 18 U.S.C. §§ 2710-11 (1994).

76. *See* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 770-73 (1999) (commenting that the market-based treatment of personal data privacy might change).

77. Larry Lessig refers to technical "code" as law. *See* LARRY LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999).

78. *See id.*; *see also* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 898 (1996) [hereinafter Lessig, *Constitution in Cyberspace*] (discussing the use of computer code as a regulatory tool or constraint on the use of a document or program); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 929 (1996) [hereinafter Reidenberg, *Governing Networks*] ("State governments can and should be involved in the establishment of norms for network activities, yet state governments cannot and should not attempt to expropriate all regulatory power from network communities."); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553, 555 (1998) [hereinafter Reidenberg, *Lex Informatica*] (noting that "the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage"); Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARV. J.L. & TECH. 287, 296-301 (1993) (commenting on the use of technical solutions to resolve various information integrity and interoperability issues).

narrowly targeted sectoral rules, technical rules have historically developed in technical fora outside the realm of public policy discourse.[79]

2. *Interpretation.*

Beyond the divergence in implementation of the First Principles, there is also important variation in the contextual interpretation of the Principles.[80] The meaning ascribed to each of the First Principles is not harmonized at the international level. These divergent interpretations can have great significance for the structure and development of online services on the Internet. The complexity and fluidity of information processing in a global network enable participants to engage in regulatory arbitrage.[81] This means that an Internet participant might shift the location of a server or database to take advantage of more permissive interpretations. At the same time, this divergence provides challenges and opportunities for the effective protection of personal data.

At the outset, the interpretation of the very applicability of First Principles is hardly uniform, especially for clickstream data. In particular, the applicability of First Principles depends on the classification of data as "personal information." Since information traces on the Internet are rampant, the distinction between anonymous and "personal information" is, thus, particularly critical.[82] For some Internet participants' traces may never be linked to the individual Web user and the user has effective anonymity. A Web site's log files may, for instance, only identify the visitor's information service provider and not the specific visitor. However, the more broadly "personal information" is interpreted for data protection purposes, the harder anonymity is to achieve. The same Web log files could identify a visitor if the information service provider reveals the identity of its subscriber. Thus, if the interpretation is broad, data protection law will apply more widely to Internet activities and more frequently to Internet participants.

Some countries treat information about legal entities as "personal information."[83] Most limit the scope to "information relating to an identified or

79. *See* Reidenberg, *Lex Informatica*, *supra* note 78, at 554.

80. *See* BENNETT, *supra* note 10, at 111-15, 222-23; CATE, *supra* note 10, at 97-100; FLAHERTY, *supra* note 14, at 371-407.

81. *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE, *supra* note 41, at 129, 151-52 (noting that it would be very difficult to eliminate "data havens").

82. *See* Kang, *supra* note 31, at 1208-10, 1220-33 (drawing distinctions between personal and nonpersonal information and illustrating the breadth of data traces left by Internet users).

83. Iceland, Italy, Luxembourg, Norway, and Switzerland are among the countries that apply privacy protections to information about corporate entities. *See* OECD, *Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks*, OECD Doc. DSTI/ICCP/Reg (98)12/FINAL ¶¶ 143, 154, 179, 198, 226 <http://www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)12-final>.

identifiable natural person."[84] The meaning of "identifiable person," however, is variable. France and Belgium, for example, under pre-European Data Protection Directive law that remains in effect, treat data as personal information if there is any way to link the information to a natural person.[85] The United Kingdom, however, took a more restrained view and examined whether the *data user* could actually link the information to a specific person.[86] These particular interpretive subtleties are unlikely to change with the transposition of the European Directive into member state national law. Further, some countries also explicitly exclude differing types of information from the scope of coverage whether or not the data relates to an individual. Belgium's statute, for example, excludes any information published by the individual concerned.[87] In the United States, interpretations of the Fourth Amendment to the Constitution emphasize a "reasonable expectation of privacy" against government searches in the context of law enforcement, which translates into a general policy preference of excluding publicly available information from protection.[88] Statutory protections in the United States tend to address applicability in terms of activities rather than individuals. For example, the Fair Credit Reporting Act defines covered information in terms of "consumer reports" rather than identifiable individuals.[89] The Cable Communications Policy Act and the Video Privacy Protection Act each refer to "personally identifiable information," but never define the term.[90]

---

84. *European Data Protection Directive, supra* note 11, at art. 2(a).

85. *See* Commission de la protection de la vie privée, Recommandation No. 01/96 du 23 septembre 1996, Recommandation de la Commission de la protection de la vie privée à propos de l'analyse de la consommation de médicaments en Belgique basée sur des informations issues des prescriptions médicales, at 5 (noting that data cannot be considered anonymous if the person responsible for the treatment can reidentify the person concerned without an important special effort); Commission nationale de l'informatique et des libertés, Déliberation No. 97-051 du 39 juin 1997 <http:www.cnil.fr/thematic/docs/ra181a.pdf> (treating Web server log files as personal information even though the server did not have access to the actual identity of visitors); COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, DIX ANS D'INFORMATIQUE ET LIBERTÉS 42 (1988) (noting that the Commission gives a broad interpretation to the term 'nominative information' in the French law).

86. *See* U.K. DATA PROTECTION REGISTRAR, DATA PROTECTION AND THE INTERNET: GUIDANCE ON REGISTRATION (1997) <http://www.open.gov.uk/dpr/internet.htm> (discussing "identifiable information" under the old Data Protection Act); Data Protection Act, 1998, ch. 29, § 1(1) (Eng.) <http://www.hmso.gov.uk/acts/acts1998/80029—a.htm#1> (adopting definitional terms in accordance with the earlier Guidance),.

87. Loi du 8 decembre 1992, art. 3, § 2.

88. *See, e.g.*, United States v. Miller, 425 U.S. 435, 437 (1976) (holding that individual lacked Fourth Amendment interest in bank records). Congress responded to the Supreme Court's decision in *Miller* with the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1994).

89. *See* 15 U.S.C. § 1681a(d)(1) (1994).

90. The Cable Communications Policy Act indicates only that "aggregate" data which "does not identify particular persons" is excluded from the definition. *See* 47 U.S.C. § 551(a)(2)(A) (1994). The Video Privacy Protection Act, however, merely states that the term includes information that identifies a person as having requested specific video materials. *See* 18 U.S.C. § 710(a)(3) (1994).

The interpretation of the transparency element of the First Principles also varies significantly across countries. Transparency requires that the processing of personal information be open and understandable. Yet, the precise meaning of this element is inconsistent in different places. Belgium, for example, required that individuals be informed of the details of the use of personal information prior to collection. In particular, the purpose for collection, also termed the finality of data use, must be disclosed with specificity.[91] The Belgian courts have interpreted this requirement strictly, ruling, for example, that a general statement disclosing that personal information will be used to provide financial services and better service to the client is insufficient to cover the use of the information in insurance solicitations.[92] The notice must be provided prior to collection of personal information if the collection is directly from the person concerned; otherwise the notice must be provided contemporaneously with the storage of the personal information.[93] France only required notification from those collecting information directly from individuals. Further, the French notification must contain a specific set of details, including whether the information must be given and what consequences follow in the absence of a response.[94] In contrast, U.S. law does not generally impose an obligation to inform individuals that data about them is being collected. However, a number of targeted statutes do require that individuals be informed prior to the dissemination of certain personal information to third parties, namely video rental records,[95] credit reports for nonstatutorily permitted purposes,[96] telephone records,[97] and cable subscription records.[98]

Oversight of information privacy is also handled in many different ways. Data protection supervisory agencies are a common feature in democracies,[99] but agency powers are often specific to each country. Some countries, for example, established regulatory enforcement agencies and licensing boards, while others adopted an ombudsman position.[100] Within the European Union, the European Data Protection Directive mandates that each Member State create an independent supervisory agency to monitor the application of

91. *See* Trib. Comm. Anvers, 7 juillet 1994, *reprinted in* 4 Droit de l'informatique et des télécomms 52-53 (1994).

92. *See id.*

93. Loi du 8 decembre 1992, art. 4(1), 9.

94. Loi No. 78-17 du 6 janvier 1978, art. 27 <http://www.cnil.fr/textes/text02.htm>.

95. *See* 18 U.S.C. § 2710(b) (1994).

96. *See* 15 U.S.C. § 1681b(a)(2) (1994).

97. *See* 47 U.S.C. § 222(c), 222(e) (1997).

98. *See* 47 U.S.C. § 551(c) (1994).

99. For discussions of different supervising models see BENNETT, *supra* note 10, at 158-92; FLAHERTY, *supra* note 14, at 11-16.

100. *See, e.g.*, Mayer-Schonberger, *supra* note 2, at 228.

data protection laws and to investigate violations.[101] In contrast, the United States has repeatedly rejected an agency enforcement model for privacy oversight, favoring industry self-regulation.[102]

In order for the national supervisory agency to monitor compliance with data protection requirements and to assure that the processing of personal information is not done secretively, European countries require public notification of data processing activities to the national supervisory agencies.[103] Nevertheless, the content of the notifications among European countries has not been uniform. Although the European Data Protection Directive stipulates the minimum information that must be filed,[104] existing European national laws have small but significant variations that are likely to persist.[105] France requires that the origin of personal information be included on the public notification, while Belgium does not, and the United Kingdom requires a textual description in connection with declarations of Internet activities involving personal information.[106] In the United States, there is no obligation to disclose the existence of data processing activities to a government agency; any such obligation would run counter to the U.S. constitutional tradition, which is suspicious of such government intrusions.[107] Only the Fair Credit Reporting Act contains a general obligation to notify the public through newspaper advertisements of the treatment of personal information, and its requirement concerns only one specific use of credit report information—the sale of names for junk mail solicitations.[108]

The substantial differences in interpretation demonstrate that First Principles have significant idiosyncratic national features. Along with the varying implementations of First Principles, these divergences take on a critical

---

101. *See European Data Protection Directive, supra* note 11, at art. 28.

102. *See* Gellman, *supra* note 53.

103. *See European Data Protection Directive, supra* note 11, at art. 18.

104. *See id.* at art. 19.

105. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 127-31 (discussing important divergences on which the European Data Protection Directive is silent). The transposition of the European Data Protection Directive will allow the Member States an important "marge de manoeuvre" to interpret the standards in the Directive. Indeed, Professor Rigaux notes that the Directive has many conditional provisions that are drafted to "leave without doubt to the national and European supervisory authorities the interpretation of the text along with the courts and tribunals, and in the last instance the [European] Court of Justice." Francois Rigaux, *La vie privée, une liberté parmi les autres, in* XIXTH INT'L CONF., *supra* note 67, at 2 (translated by author).

106. *Compare* Loi No. 78-17 du 6 janvier 1978, art. 19 (France), *with* Loi du 8 decembre 1992, art. 3 (Belgium) <http://www.privacy.fgov.be/loi_vie_privée_belge.htm>, *with* U.K. DATA PROTECTION REGISTRAR, *supra* note 86.

107. *See* CATE, *supra* note 10, at 124 (noting that such a "scheme is anathema to the U.S. constitutional system"); INFORMATION POLICY COMMITTEE, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (Apr. 1997) <http://www.iitf.nist.gov/ipc/privacy.htm> (highlighting that the U.S. prefers non-regulatory solutions)

108. *See* 15 U.S.C. § 1681b(e)(5) (1994).

dimension for the Internet where competition among information privacy rules ensures confrontation and conflict.

III. ONLINE CONFRONTATION AND CONFLICTS

The lack of harmonization in the execution of First Principles poses a fundamental challenge to international data flows and the Internet. The Internet places divergent rules in proximity through architectural features that promote geographic indeterminacy. If the policies achieved by divergent executions of First Principles were "functionally similar,"[109] then international data flows would not face challenges. But, since the degree of substantive protection varies widely,[110] international data flows assure confrontation and conflict among the different national regimes for protection of personal information.

In effect, the characteristics of data transfers destabilize[111] the fair treatment of personal information. Multinational processing of clickstream information, warehoused data, and the pressures for secondary use, in particular, place the legal rules, data protection policies, and information practices of various jurisdictions in direct conflict.[112] If access to, collection, and processing of personal information occur in several countries over the network, then each of the implicated countries may assert legal jurisdiction.[113] At the same time, multiple regulatory regimes attenuate the enforcement jurisdiction of each country.[114] This paradox is not readily

109. This term refers to the search by comparative law scholars to find similarity in the substantive results across different countries rather than identity of legal instruments in different legal cultures. *See* Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data, Annex to the Annual Report 1998 of the Working Party Established by Art. 29 of Directive 95/46/EC, Eur. Comm. Doc. No. XV D/5047/98 (1998) <http://www.droit.fundp.ac.be/crid/privacy/Tbdf/Chapitre1.pdf>; SCHWARTZ & REIDENBERG, *supra* note 9, at 24-25 (describing use of "functional similarity" analysis to compare U.S. and European data protection practices).

110. *See generally* CATE, *supra* note 10; SWIRE & LITAN, *supra* note 10; Mayer-Schonberger, *supra* note 2; *Existing Case-Law on Compliance with Data Protection Laws and Principles in the Member States of the European Union, Annex to the Annual Report 1998 of the Working Party Established under Article 29 of Directive 95/46/EC*, E.C. DOC. XV D/5047/98 (Douwe Korff ed., 1998) [hereinafter *Existing Case-Law*].

111. *See* notes 16-34 *supra* and accompanying text.

112. Robert Gellman writes that the uncertainty of legal rules for interactions on the Internet results in conflicting and overlapping privacy laws and rules. *See* Gellman, *supra* note 41, at 272-77.

113. *See* Henry H. Perritt, Jr. *Jurisdiction in Cyberspace: The Role of Intermediaries, in* BORDERS IN CYBERSPACE, *supra* note 41, at 164 (examining the jurisdictional problems that the Internet presents); Jon Bing, *Data Protection: Jurisdiction and the Choice of Law, in* PROC. XXI INT'L CONF, *supra* note 44 (analyzing jurisdictional and choice of law problems for data protection law).

114. *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1216-21 (1999) (arguing that the threat of liability for individual users is far less than what many commentators have suggested because of the difficulty of establishing jurisdiction over the users).

resolved by traditional "conflict of law" principles.[115] The overlapping and malleable nature of international data flows present a basic challenge to the localization required for choice of law analysis.[116] Multiple laws may apply to an unique activity. In terms of substantive conflicts, a number of key problems arise.

A. *Implementation and Systemic Legal Conflict*

The most well-known conflicts arise from systemic differences in the approach and the specific content of data protection rights.[117] In Europe, comprehensive data protection laws establish rights and obligations for the treatment of personal information.[118] Elsewhere, information privacy may be assured by narrower legal rules, policies or practices, or alternatively, data protection may even be ignored.[119] In the absence of comprehensive data protection legislation, the full range of internationally-recognized principles for fair information practice may be hard to satisfy; narrow, sectoral laws, policies, ad hoc protections and practices typically ignore key elements of the First Principles.

If data protection is taken seriously, then systemic legal conflicts should cause disruption of international data flows.[120] Both the European Union's Data Protection Directive and existing European Member State laws provide for the prohibition on data flows to countries without satisfactory privacy protection.[121] For the United States alone, Europe has justification to restrict the processing of European personal information; U.S. legal rights are too narrow and too rare, while the U.S. reliance on self-regulation has proven

---

115. *See id.* at 1210 (discussing the dichotomy between default and mandatory rules along with the problem of spillover effects).

116. *See* Bing, *supra* note 113.

117. *See* Working Party Established under Art. 29 of Directive 95/46/EC, *Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, E.C. DOC. XV D/5020/97–WP 4 (June 26, 1997) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp4en.htm> [hereinafter Working Party, *First Orientations*]; Working Party Established under Art. 29 of Directive 95/46/EC, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, E.C. DOC. DG XV D/5025/98WP 12 (July 24, 1998) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp12en.htm> [hereinafter Working Party, *Transfers of Personal Data*].

118. *See European Data Protection Directive*, *supra* note 11.

119. *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 24-25 (discussing U.S. data privacy regime).

120. *See, e.g.*, Ulf Brühann, *Data Protection in Europe: Looking Ahead*, *in* PROC. XIXTH INT'L CONF., *supra* note 67, at 3-4 ("Nobody should underestimate the problem by doubting the political will of the European Union to protect the fundamental human rights of citizens.").

121. *See European Data Protection Directive*, *supra* note 11, at art. 25; France, Law No. 78-17 of Jan. 25, 1978, at art. 24; *see also* Peter Blume, *An EEC Policy for Data Protection*, 11 COMPUTER/L.J. 399 (1992); Michael Kirby, *Legal Aspects of Transborder Data Flows*, 11 COMPUTER/L.J. 233 (1992); Schwartz, *supra* note 12;

ineffective in protecting privacy at the level of European standards.[122] Similar justifications exist for other countries lacking analogous laws and basic data protection rights. Thus, systemic differences in the approach and rules of national data protection regimes place each other in direct conflict.

B. *Interpretation and Detail Conflict*

In addition to systemic conflicts, online services face another important risk to international data flows. Seemingly minor divergences in the laws of several countries have significant ramifications for international data flows of personal information.[123] For example, slight differences in the requirements for the contents of notification to individuals prior to the collection of their personal information mean that data collectors cannot use the same notice for residents of different jurisdictions.[124] Since the network environment obscures the location of users, data collectors often face a difficult choice: Either they ignore the requirements of countries where data collection might be taking place or they unwittingly contravene these requirements. These conflicts of divergence become particularly pronounced for intracorporate data-sharing arrangements and for emerging electronic commerce activities.[125]

C. *Compliance and Conflict*

Beyond conflicts created by systemic differences and interpretive divergences, compliance deficiencies within a national framework may lead to claims of discrimination. For example, many European websites surreptitiously capture information about their visitors in violation of local data protection laws;[126] in the United States, an FTC study of online services reported

122. *See* SCHWARTZ & REIDENBERG, *supra* note 9 (demonstrating the significant weaknesses in U.S. privacy law and practice as compared to European principles); Reidenberg, *supra* note 57 (arguing that U.S. privacy protection has poor results); U.S. DEP'T OF COMMERCE, DRAFT INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES (Nov. 15, 1999) <http://www.ita.doc.gov/ecom/Principles1199.htm> (proposing a privacy accord between the United States and the European Union that implicitly recognizes the inadequacy of U.S. law). *But see* SWIRE & LITAN, *supra* note 10 (arguing that U.S. data privacy law is sufficient).

123. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 139-49 (discussing the impact of conflicts on online services and the role of the uniform choice of law rule in the European Directive).

124. If notice requirements do not conflict, then it would be possible, though cumbersome, to aggregate all notice elements of all relevant laws into one detailed notice.

125. *See, e.g.*, *Processing of Personal Data*, *supra* note 68; SWIRE & LITAN, *supra* note 10, at 60-64.

126. Among the notable examples: In Belgium as of August 5, 1997, none of the major online service providers (MSN, Skynet, CompuServe, Datapak and Interpac) had complied with the registration requirements of Belgian law. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 195. In Germany, also in 1997, the websites of *Der Speigel* and Kaufhof (a major department store) each failed to disclose their information practices in violation of German law, *see id.* at 77, and in France, La Redoute (a major online retailer) uses "cookies" and fails to disclose its practices in

dismal adherence to even minimal standards of fair information practice in 1998.[127] In Spain, the small number of transfer requests made to the data protection authority must be disproportionately small when compared to the reality of data exports.[128] This gap between data protection principles and actual practice transforms the terms of international debate on the protection of personal information. In the international context, instead of focusing on the quality of protection afforded to personal information, the debate becomes one of unfair discrimination.[129] If compliance is a problem in a country, then to hold foreign data processors to a higher level of actual practice is discriminatory. The wider the national gap between principle and practice, the stronger the claim of discrimination if the principles are only applied stringently to international data flows.

IV. GOVERNANCE CHOICES AND INFORMATION PRIVACY LAWS

Over the years, the conflicts have led to several major international efforts at harmonization of information privacy standards. Indeed, the Organization for Economic Cooperation and Development (OECD) Guidelines and the Council of Europe Convention were pre-Internet responses to the growing disparity in treatment of personal information around the world. As Professor Charles Raab has astutely observed, however, "implementation differences coupled with national differences in administrative use of personal data and in the configuration of commercial competitive positions in international trade have made harmonization difficult to achieve even when confined only to the European Union."[130] Just within the context of Europe's online environment, the European Data Protection Directive is unlikely to

violation of French law. *See La Redoute* <http://www.laredoute.fr/>. Despite the obviousness of these violations, none of the companies have been prosecuted for violations of the national laws.

127. *See* PRIVACY ONLINE, *supra* note 46; *see also* SELF-REGULATION, *supra* note 46 (reporting that fewer than 14% of websites' privacy notices comply with the FTC's set of standards for notice and choice). One year later, a study conducted at Georgetown University found that 65.9% of the commerical websites sampled in the study posted some form of privacy disclosure. *See* Mary J. Culnan, *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*, at 10 (June 1999) <http://www.msb.edu/faculty/culnanm/GIPPS/mmrpt.PDF>. But only 13.6% of these sites had a complete policy. *See id.* at 10.

128. During 1997, only 793 international transfers were declared to the Spanish data protection agency. *See* Agencia de Proteccion de Datos, *International Data Transfers*, at 4 (May 1997) <http://www.privacyexchange.org/tbdi/tbdistudies/spaindt97.html>.

129. *See, e.g.*, Joel R. Reidenberg, *The Globalization of Privacy Solutions: The Movement towards Obligatory Standards for Fair Information Practices*, *in* VISIONS OF PRIVACY, *supra* note 51, at 219-20 ("Any European restrictions on the flow of personal information must, thus, satisfy the tests of non-discrimination among third countries."); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 50 (2000).

130. *See* Raab, *supra* note 42, at 168.

achieve the goal of full harmonization.[131] These efforts, nevertheless, strengthen the policy convergence on First Principles.

The consensus on First Principles of fair information practice and the search for harmonized rules obscure the intrinsic connection between governance and fair information practices. Professor Colin Bennett, in his pioneering work, attributes the degree of convergence on First Principles and recent harmonization efforts to several forces: (1) common features of information technology; (2) an elite network of policy activists; and (3) European restrictions on transborder data flows.[132] Bennett explains well the political influences on the policy-making process and the universality of First Principles. But, he limits his analysis to the "policy toolkit"[133]—the choice of instruments to achieve First Principles—and finds political explanations for the choice of different policy instruments.

This Part argues, instead, that the national differences are more profound than the politics leading to the choice of policy instruments. Rather, the divergence in execution derives from fundamentally distinct visions of democratic governance. Democratic countries do not share the same traditions and views on the role of the state in protecting the rights of citizens and the ability of the market to assure the fair treatment of citizens. In these societal balances, information privacy rules have an essential and normative governance function.[134] Indeed, the distinct executions of First Principles show that particular information privacy rules either help to shape a liberal, self-reliant governance balance or help to establish a socially-protective governance balance.

A. *The Normative Role of Privacy in Democratic Governance*

Privacy is an essential feature of a citizen's ability to participate fully in democratic society.[135] László Majtényi, the Hungarian Parliamentary Com-

131. *See European Data Protection Directive*, *supra* note 11, at Recitals 7-8 (defining goal of harmonization); REIDENBERG & SCHWARTZ, *supra* note 43, at 123-46 (arguing that important divergences in European national laws will persist after the transposition of the European Directive).

132. *See* BENNETT, *supra* note 10, at 220-50; *see also* Bennett, *supra* note 2.

133. *See* BENNETT, *supra* note 10, at 194.

134. Bennett argues that "each national choice reflects something about the political system in question." BENNETT, *supra* note 10, at 192. This section, however, seeks to show that the connection between the execution of First Principles and national politics is normative rather than derivative.

135. *See* Raab, *supra* note 42, at 161-65 (noting that data privacy is a necessary protection in a democratic state); Jeb Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989) (arguing that privacy is a basic right of citizens); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 555 (1995) (arguing that data privacy is necessary for public participation in government); Simitis, *supra* note 42, at 732-37 (arguing that privacy is essential for citizens to exercise freedom in a democratic society).

missioner for Data Protection and Freedom of Information, observed as his country moved from Eastern European communism to Western European democracy that "nearly every case we handle has to do, in one way or another, with constructing the constitutional state."[136] As such, privacy rights play a normative role in democratic governance. These rights delineate the boundary of state control over individuals and define the basic attribute of citizenship.

Privacy is often cast as an individual's desire for seclusion from the public realm. Samuel Warren and Louis Brandeis made this strain of privacy famous in their argument for a "right to be let alone."[137] This conception of privacy implicitly articulates a particular vision of the individual's liberty in society, namely that the individual should have the ability to withdraw and to associate with others. This also shows that privacy rights define relationships among citizens.[138]

Competing theories of privacy are more direct in the link between privacy and governance. The autonomy theory of privacy argues that individuals have the right to define themselves for others and specifically interprets privacy as necessary for political participation.[139] This "right to control the disclosure of personal information to others" sets the framework for private social interaction as well as political interchange.[140] The dignity theory calls for privacy protection as a means for individuals to ratify their identity and self.[141] In effect, the protection of dignity would broadly set the constitutional ground rules for an individual's interactions with others. Lastly, civility theory sees privacy as protection for community boundaries of decency.[142] Perhaps most directly, civility presents privacy as a key instrument of social governance.

In a networked environment, individual identity and liberty are linked intrinsically to the treatment of personal information.[143] Data privacy rules are often cast as a balance between two basic liberties: fundamental human

136. Lásló Majtényi, *Data Protection in the Era of Change of the Political System*, *in* PROC. XIXTH INT'L CONF., *supra* note 67, at 3.

137. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-96 (1890).

138. *See also* Schwartz, *supra* note 47, at 68 (arguing for "information territories" to define relationships).

139. *See* WESTIN, *supra* note 14.

140. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).

141. *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 965-66 (1964).

142. *See* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 957 (1989) (arguing that the invasion-of-privacy tort protects rules of civility but that the expansion of mass media poses an important threat to the rules).

143. *See* Herbert Maisl, *Etat de la legislation francaise et tendence de la jurisprudence relatives a la protection des donnees personelles*, 1987 Rev. int'l de droit compare 559.

rights on one side and the free flow of information on the other side.[144] Yet, because societies differ on how and when personal information should be available for private and public sector needs,[145] the treatment and interaction of these liberties will express a specific delineation between the state, civil society, and the citizen.

B. *Liberal Norms and Data Privacy*

The liberal state emphasizes limits on government power and is characterized by its hostility toward the regulation of private relations. In Lockean terms, the role of the state is to protect property[146] and the state is a force to be restrained.[147] For privacy, the liberal approach prefers private rights[148] and regards the state with suspicion.[149] In this context, personal information needs to be protected from interference. State regulation should be sparse and as narrowly constructed as possible. To the extent that the free flow of information promotes private activity and autonomy, private contract, rather than state regulation becomes the source of regulation for information. Individuals must vindicate their own rights.

The United States conceives of its democracy as such a liberal state. The U.S. Constitution synthesizes commitments to self-governance and individual rights.[150] With these commitments, there is a strong anti-statist element. Indeed, there is an ideological hostility to regulation of private relations despite the rise of the social welfare state in America.[151] For information flows, there is a reflexive impulse against any restrictions on the treatment of personal information.[152] This draws on the powerful First Amendment tradition in the United States.

---

144. *See* Rigaux, *supra* note 105, at 3.

145. *See* Herbert J. Spiro, *Privacy in Comparative Perspectives*, *in* PRIVACY NOMOS XIII 121-22, 128 (J. Roland Pennock & John W. Chapman eds., 1971) (noting that Americans more readily share personal information with private organizations than government while continental Europeans do the reverse and arguing that Germany and the United States are at polar positions with respect to privacy while England falls in the middle).

146. JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT 70–73 (Thomas P. Peardon ed., Liberal Arts Press 1952) (1690).

147. *See id.* at 75-82.

148. *See, e.g.*, David W. Leebron, *The Right to Privacy's Place in the Intellectual History of Tort Law*, 41 CASE W. RES. L. REV. 769, 785-88 (1991) (discussing the liberal antimajoritarian emphasis of Brandeis' approach to privacy).

149. *See, e.g.*, Spiro, *supra* note 145, at 129-31.

150. *See* Martin S. Flaherty, *History "Lite" in Modern American Constitutionalism*, 95 COLUM. L. REV. 523, 579-90 (1995).

151. *See* Morton J. Horwitz, *The History of the Public/Private Distinction*, 130 U. PA. L. REV. 1423, 1424 (1982) (arguing that it was the development of the economic market in the nineteenth century that brought the public/private distinction into focus for the legal community).

152. *See* Reidenberg, *Setting Standards*, *supra* note 36, at 502-04.

For the execution of First Principles, the liberal commitment has particular significance. Specifically, liberal politics are concerned with coercive state behavior.[153] Sectoral rather than omnibus laws minimize state intrusions on information processing. Sectoral laws, such as the Fair Credit Reporting Act,[154] react to specific problems and provide only narrow state intervention to protect privacy. For information privacy, this also means that the public sector and police powers, rather than private conduct, are suspect.

The scope of legal protection executing First Principles under liberal norms as seen in the Untied States is quite narrow. The political philosophy of nonintervention translates into a narrow definition of personal information. Discussion in the United States tends to exclude public record information from protection as "personal information."[155] This narrow definition, in effect, places a limit on the state's power to regulate information privacy. At the same time, the focus of any information privacy legislation will be very narrow. Not surprisingly, in the United States, law targets discrete information processing activities and the most important legislative protections for information privacy emphasize restraint on government. The Privacy Act of 1974,[156] the Freedom of Information Act of 1974,[157] the Right to Financial Privacy Act of 1978,[158] and the Electronic Communications Privacy Act of 1986[159] are exclusively or predominantly about the treatment of information by the government.

Of equal importance under liberal theory is that markets, rather than law, shape information privacy. Privacy is conceived as a fully alienable commodity and individual autonomy depends on the ability to make atomistic decisions about the sale of personal information. Regulation is perceived to intrude on the commitment to freedom from government interference in information flows.[160] As a result, law emphasizes regulation of the market process rather than the substantive contours of information privacy. The expectation is that the market will then execute the First Principles. This market emphasis means that transparency should be the prime regulatory focus.[161] In the United States, for example, there are few legal restrictions on

153. *See* LOCKE, *supra* note 146, at 112-18 (describing tyranny as power beyond right).

154. 15 U.S.C. § 1681 (1998).

155. *See, e.g.*, SWIRE & LITAN, *supra* note 10, at 36 (noting the broader scope of public records in the United States); McHugh, *supra* note 38, at 188-89 (citing Yahoo!'s chief marketing officer's rationalization that Yahoo!'s user profiles are not personal information).

156. 5 U.S.C. § 552a (1996).

157. 5 U.S.C. § 552 (1996).

158. 12 U.S.C. §§ 3401-3422 (1994).

159. 18 U.S.C. §§ 2510-2522, 2701-2711 (1994).

160. *See, e.g.*, CATE, *supra* note 10, at 68-72.

161. Cate notes that a key feature of public sector privacy laws "is the emphasis, carried over from First Amendment jurisprudence, on ensuring widespread access to data to support democratic self-governance." *Id.* at 76.

the collection, storage, or dissemination of information.[162] The absence of law also encourages the rise of information policy rules through technical code.[163] These technical rules embed information privacy decisions, or more often privacy violations,[164] in network architecture. Ultimately, they leave the rule-making to private standards groups such as the Internet Engineering Task Force[165] and the World Wide Web Consortium.[166]

For the market approach, three issues are of paramount importance: notice, consent, and accuracy. In the United States, the sectoral statutes tend to address accuracy of information.[167] But, they do not give broad access to personal information held by others. For example, there is no legal right in the United States for an individual to compel Acxiom[168] to reveal the personal information that Acxiom sells about the inquiring person. This narrow construction of the First Principle calling for rights of access[169] favors the interests of those holding information about others. In staying true to Locke, the narrow construction protects the effort of the collector of personal information.

With respect to notice and consent, U.S. government policy stresses these two elements of First Principles.[170] Yet, the execution of these elements generally remains outside the boundaries of law and is left to the marketplace. The anti-state perspective disdains government interference in

---

162. *See* Reidenberg, *Setting Standards*, *supra* note 36, at 528-29.

163. *See* LESSIG, *supra* note 77; Reidenberg, *Lex Informatica*, *supra* note 78.

164. Richard Smith, a technical expert, has, in pioneering work, identified the privacy invasive architectures of a number of popular products such as the fingerprinting of Microsoft Office 97 files with a Global Unique Identifier (GUID) and Internet design features such as Web bugs that preclude anonymous browsing. Richard M. Smith, *Internet Privacy Issues* <http://www.tiac.net/users/smiths/privacy/>.

165. The Internet Engineering Task Force is, for example, working on IPv6, a protocol for internet addressing, that will require a unique identifier for each machine connected to the Internet. *See* Thomas Narten & R. Draves, *Privacy Extensions for Stateless Address Autoconfiguration in Ipv6*, at § 2 (Oct. 1999) <http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-addrconf-privacy-01.txt>.

166. W3C has sought to develop a number of technological privacy tools such as the Platform for Internet Content Selection (PICS) and the Platform for Privacy Preferences (P3P). The W3C Web site is at <http://www.w3c.org>.

167. *See, e.g.*, 15 U.S.C. § 1681i (1994) (Fair Credit Reporting Act error correction requirement); 15 U.S.C. § 1693(f) (1994) (Fair Credit Billing Act error correction requirement); Preservation of Records of Communication Common Carriers, 51 Fed. Reg. 32653 (1986) (to be codified at 47 C.F.R. pt. 42) (telephone billing regulations providing for dispute procedures).

168. Acxiom is one of the largest companies in the United States selling personal information to direct marketers. *See Axciom* <http://www.acxiom.com>.

169. *See* text accompanying note 51, *supra*.

170. *See, e.g.*, THE WHITE HOUSE, *supra* note 8, at Issue 5 ¶4 (stating that "principles of fair information practice [] rest on the fundamental precepts of awareness and choice"); PRIVACY WORKING GROUP, U.S. DEP'T OF COMMERCE, *supra* note 30 (relying principally on notice and choice as the privacy paradigm for the Information Age).

consensual decisions.[171] The most recent privacy legislation, contained in the Financial Services Modernization Act,[172] allows rampant sharing of personal information among corporate affiliates provided consumers are informed periodically that their privacy will be violated. This approach willfully ignores "public order" considerations such as the validity of consent for certain types of processing activity.[173]

Next, the American liberal philosophy minimizes execution of the First Principle of finality. Purpose limitations on the use of collected personal information are seen as contrary to the ideology of free flows of information.[174] In fact, one of the few statutes to impose purpose limitations on the use of personal information, the Fair Credit Reporting Act,[175] interprets the purposes compatible with the rationale for collection broadly. The Fair Credit Reporting Act explicitly allows the use of credit report for certain marketing purposes; namely, to make unsolicited credit and insurance offers.[176]

Significantly, the American commitment to liberal values for information flows is supported by the absence of public enforcement mechanisms for First Principles. The sparse existence of legal rights proffers few judicial remedies and there is no Data Protection Commission in the United States. The state does not act as the direct protector of citizens. Instead of public sanction, private initiative offers the principal means of enforcement of fair information practices. By relying on private action, citizens must vindicate their own interests and the opportunities for state interference with information privacy are limited.[177]

---

171. Indeed, the U.S. Constitution also prohibits state interference with private contract. *See* U.S. CONST. art. I, § 10, cl. 1 ("No State shall . . . pass any . . . Law impairing the Obligation of Contracts."); Trustees of Dartmouth College v. Woodward, 17 U.S. 518 (1819) (voiding the New Hampshire legislature's attempt to modify a private college's charter).

172. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338.

173. For years, U.S. law has ignored the legitimacy of a patient's consent to the sharing of medical information as a condition for insurance payment. A typical medical insurance form includes language such as the following: "I authorize any Health Care Provider, Insurance Company, Employer, Person or Organization to release any information . . . to any CIGNA company, the Plan Administrator, or their authorized agents for the purpose of validating and determining benefits payable." Cigna HealthCare Group Medical Direct Reimbursement Claim Form (CL505517 2-96) (on file with the *Stanford Law Review*). The release includes no obligation for CIGNA to keep the information confidential, nor does it preclude CIGNA from using any acquired information for other purposes. These terms are not negotiable.

174. *See* CATE, *supra* note 10, at 99 ("Privacy laws in the United States most often prohibit certain disclosures, rather than collection, use, or storage, of personal information.").

175. 15 U.S.C. § 1681 (1998).

176. *See* 15 U.S.C. § 1681b(c) (1998).

177. U.S. rhetoric typically refers pejoratively to any privacy regulator as a "czar." *See, e.g.*, Remarks of Ambassador David L. Aaron, Under Sec'y of Comm. for Int'l Trade, U.S. DEP'T of Comm., before the World Affairs Council Panel on the WTO & E-Commerce, Seattle, WA 3 (Nov. 12, 1999) <http://www.ita.doc.gov/media/EWTO1112.htm>; Remarks of David L. Aaron, Under-

By design, in this liberal approach, law is ad hoc and reactive. Faced with rapidly changing, technologically driven uses of personal information, the execution of many of the First Principles tends to fall by the wayside.[178] Sectoral regulation is circumvented by cross-sectoral information processing and key areas are intentionally ignored. Indeed, sectoral borders themselves may be impossible to define.[179] Non-economic values such as human dignity do not enter into the calculus. At the same time, key conditions necessary for the market to successfully account for privacy interests are missing.[180] Basic transparency and informed consent are far from the reality in the United States.

The nonexecution of First Principles in the United States leads to an interesting network effect.[181] Few restraints on information trafficking have allowed an enormous volume of personal information to be collected and disseminated. For those who seek customized products, the larger volume of personal information in circulation gives business a greater ability to develop those products.[182] But, there is an important externality: It becomes harder for individuals to maintain information privacy as more information about others circulates. Profiling and inferential predictions based on aggregate information affect each individual.[183] The collective market treatment of personal information restrains any individual's decisionmaking freedom.

While liberal objectives might be frustrated by the suppression of individualism through market-dominated decisionmaking, the execution of First Principles in the United States clearly enshrines a liberal philosophy. Whatever criticism might be made regarding the sorry state of information privacy in the United States, the free market, self-regulatory approach adopts governance choices in the United States.

---

sec'y of Comm. for Int'l Trade, U.S. Dep't of Comm., before the Information Technology Association of America Fourth Annual IT Policy Summit, Washington, DC 2 (Mar. 15, 1999) <http://www.ita.doc.gov/media/Itaapr31599.htm>

178. *See* Reidenberg, *supra* note 57, at 775-76, 779-80 (describing market failure and missing elements of fair information practice); Schwartz & Reidenberg, *supra* note 9, at 338-90 (showing lack of transparency).

179. *See* Reidenberg, *Governing Networks*, *supra* note 78, at 915-17 (discussing the breakdown of borders between substantive bodies of law); Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Rules*, 41 VILL. L. REV. 129, 143-45 (1996) (noting overlaps in sectoral industry codes of conduct).

180. *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997) (arguing that the operation and economics of complex economic markets, health care and employment for example, actually favor data privacy protection).

181. *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998).

182. *See* Samarajiva, *supra* note 19, at 278-81. "In sum, mass customization requires the surveillance of spatially dispersed, dynamic target markets and the building of relationships with customers. Customized production goes with customized marketing, which goes with customer surveillance. This is the surveillance imperative." *Id.* at 279.

183. *See* Simitis, *supra* note 64, at 726-29.

C. *Social-Protection Norms and Data Privacy*

In contrast to the United States' liberal philosophy, other democracies, typically European, approach information privacy from the perspective of social protection. Under this governance philosophy, public liberty derives from the community of individuals and law is the fundamental basis to pursue norms of social and citizen protection.[184] This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop,[185] and information practices must serve individual identity.[186] Citizen autonomy, in this view, effectively depends on a backdrop of legal rights.

In this context, data privacy is a political imperative anchored in fundamental human rights protection.[187] Citizens trust government more than the private sector with personal information.[188] Consequently, European democracies approach data protection as an element of public law.[189] Louise Cadoux, former Vice President of the French National Commission on Data Processing and Liberties, succinctly notes: "[F]or Europe, the choice is clear: privacy protection is an exclusive issue of law."[190]

---

184. *See* LAURENT COHEN-TANUGI, LE DROIT SANS L'ETAT: SUR LA DEMOCRATIE EN FRANCE ET EN AMERIQUE 10 (1985) (noting that the American model of "a 'contractual society' opposes naturally the other great model of regulation, the Social Contract, a meta-contract uniting the entire society to the creation of a State by a general and absolute delegation of power from the former to the second") (translation by author).

185. *See* Rigaux, *supra* note 105 (arguing that privacy is one of several competing freedoms that must be decided on by the legislature); Yves Poullet, *Data Protection Between Property and Liberties: A Civil Law Approach, in* AMONGST FRIENDS IN COMPUTERS AND LAW 170-71, 175 (H.W.K. Kaspersen & A. Oskamp eds., 1990) (noting that civil law looks to create fundamental privacy rights).

186. As an example, the very first sentence of the French data privacy law is "computer processing must serve the citizen." *See* Law No. 78-17 of Jan. 6, 1978, at art. 1 <http://www.cnil.fr/textes/text02.htm>.

187. *See* COE Convention, *supra* note 14, at preamble & art. 1. The Convention provides:

> Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing .... [Art. 1] The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Id.

188. *See* Spiro, *supra* note 145, at 122.

189. *See generally* T. Koopmans, *Privacy and the Dilemmas of Human Rights Protection, in* PROC. XVITH INT'L CONF. DATA PROT. COMM'RS 72, 72-77 (Sept. 1994) <http://cwis.kub.nl/~dbi/regkamer/proc.htm> [hereinafter XVITH INT'L CONF.] (discussing the development of data protection in European jurisprudence); Peter Blume, *Legal Culture and the Possibilities of Control, in* 3 LECTURES ON DATA PROTECTION 19, 35 (1992).

190. Louise Cadoux, *Autoroutes de l'information et vie privee: ethique, auto-regulation et loi, in* PROC. XIXTH INT'L CONF., *supra* note 67 (translated by author).

To assure social protection, data protection norms in Europe interpose the state in creating parity between organizations and individuals. France and the European Data Protection Directive, for example, prohibit the use of purely automated decisions about citizens.[191] This socially-protective approach to regulation seeks to manage relationships and fully execute First Principles. Law, thus, enshrines prophylactic protection through comprehensive rights and responsibilities.[192] The scope of coverage is expansive. European data protection laws are cross-sectoral, affecting all industries and the public sector.[193] Indeed, the commitment to free flows of information is far narrower than in the liberal approach. For example, in the interest of assuring freedom of speech, European journalists enjoy some exceptions to the rules for processing personal information.[194] But, these exceptions are weaker than the First Amendment protections afforded to journalists in the United States, where virtually any restriction will be attacked as unconstitutional.[195]

Under the social-protection approach, the execution of First Principles emphasizes the legitimacy of processing personal information. Not surprisingly, European law rejects consent as an absolute basis for the treatment of personal data.[196] In addition, European law insists on the "fair[] and lawful[]"processing of personal information.[197] The interpretation of legitimacy will, however, be circumscribed by the extent of the social protection sought. For example, the United Kingdom and Germany, until transposition of the European Data Protection Directive, did not explicitly control the processing of sensitive data,[198] while France and Belgium did.[199] These latter countries

---

191. *See* Law No. 78-17 of Jan. 6, 1985, 1978 <http://www.cnil.fr/textes/text02.htm>; *European Data Protection Directive*, *supra* note 11, at art. 15(1).

192. *See* SWIRE & LITAN, *supra* note 10, at 22-31 (discussing the application of the European Directive's privacy protections in Europe); Schwartz, *supra* note 12.

193. *See European Data Protection Directive*, *supra* note 11, at recital 12, art. 3(1).

194. *See id.* at art. 9 ("Member States shall provide for exemptions . . . for the processing of personal data carried out solely for journalistic purposes . . . .").

195. *See* SWIRE & LITAN, *supra* note 10, at 31 ("The use of 'only' and 'necessary' suggest that free expression will prevail over privacy rights less often than would be true under the First Amendment to the U.S. Constitution."); Jane Elizabeth Kirtley, *Privacy and the News Media: A Question of Trust, or of Control?*, *in* PROC. XXIST INT'L CONF., *supra* note 44 (criticizing the European Data Protection Directive as restrictive of press freedoms)

196. *See European Data Protection Directive*, *supra* note 11, at art. 8 (requiring protection for sensitive data).

197. *See id.* at art. 6.

198. The U.K. Data Protection Act of 1984 allowed the Secretary of State to issue regulations for four types of sensitive data, but none were ever issued. *See* Data Protection Act, 1984, § 2(3) (Eng.). The German law incorporated higher protection of sensitive data through a balancing clause. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 96-97.

199. *See* COMMISSION DE PROTECTION DE LA VIE PRIVÉE, 1996 RAPPORT D'ACTIVITE 38 (1997) (noting that advance consent is required for processing sensitive data in Belgium); Law No. 78-17 of Jan. 6, 1978, at art. 31 <http://www.cnil.fr/textes/text02.htm>.

had, perhaps, a stronger tradition of state paternalism than the United Kingdom or Germany.

Finality is similarly a key element of social protection. European data protection law places a critical finality restriction on the processing of personal information.[200] To assure the enforcement of First Principles, public oversight mechanisms also embody the social protective approach. European data protection law establishes powerful state supervisory agencies.[201] Indeed, Denmark even calls its public agency the "Data Surveillance Authority."[202] These agencies accomplish their mission through declaratory schemes and licensing.[203] Criminal sanctions are also a feature of public enforcement in many states.[204] These contrast dramatically with the liberal approach, which eschews such deep state involvement in the regulation of information flows.

Although social-protection norms pervade the execution of First Principles in European democracies, divergences do exist.[205] The scope of coverage of data protection laws is broader, for example, in France and Belgium than in the United Kingdom.[206] In Germany, there is even an explicit mandate to provide anonymous and pseudonymous online interactions.[207] These diverging scopes appear to reflect the respective political cultures of state involvement in the private sector; France and Belgium have a Colbertist tradition of governance, whereas the United Kingdom is more independent and

---

200. *See European Data Protection Directive*, *supra* note 11, at art. 6 ("Member States shall provide that personal data must be ... collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.").

201. *See id.* at art. 28 ("Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States.").

202. *See Data Surveillance Authority* <http://www.registertilsynet.dk/eng/index.html>.

203. *See* BENNETT, *supra* note 10; FLAHERTY, *supra* note 14 (discussing the role, politics, and operation of data protection agencies); *European Data Protection Directive*, *supra* note 11, art. 19 (describing the information that must be provided to the supervising agency prior to a data collection).

204. *See, e.g.*, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY, OECD, INVENTORY OF INSTRUMENTS AND MECHANISMS CONTRIBUTING TO THE IMPLEMENTATION AND ENFORCEMENT OF THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS, OECD Doc. DSTI/ICCP/REG(98)12/FINAL at 18-50 (May 11, 1999) <http://www.olis.oecd.org/olis/1998doc.nsf/4cf568b5b90dad994125671b004bed59/0663f1ef6343f3a78025677d00529a52/$FILE/05E95540.ENG> (reporting on implementation of OECD guidelines and noting relevant criminal sanctions in various countries).

205. *See* FLAHERTY, *supra* note 14 (analyzing differences in public sector regulation of data privacy); REIDENBERG & SCHWARTZ, *supra* note 43 (studying divergences across several European national laws).

206. *See* notes 82-86 *supra* and accompanying text (discussing the definition of "identifiable" information).

207. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 39-40 ("The IuKDG requires service providers 'to offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable.'").

the modern German history of the Holocaust offers a compelling motive to promote anonymity. Transparency rules in Europe also include differing levels of intrusiveness for the collectors and users of personal information. The notices to individuals for the processing of personal information and the registration statements that must be filed with national supervisory authorities vary in their details.[208]

For the online context, the social-protection approach has an important conceptual appeal. The approach is cross-sectoral and inclusive; personal information receives privacy protection regardless of the processing arrangement. In contrast, the liberal approach restricts protection to increasingly irrelevant sectoral boundaries. At the same time, however, the social-protection approach poses normative challenges. The complexity of data-processing architectures on the Internet makes the application of First Principles to particular contexts difficult. An illustration of this point is found in the registration mechanisms designed to assure transparency. With respect to online services, these requirements can prove rather onerous and problematic. In fact, there is a debate as to the effectiveness of compliance and enforcement.[209] Beyond this implementation of First Principles, the interpretation of standards poses additional problems. Small divergences and ambiguities will distort the structure and flows of personal information.[210] Differences in the treatment of Internet Protocol addresses may, for example, affect where service providers locate address servers.

In the face of the growing issues of divergence with European data protection laws despite the shared governance philosophy, harmonization of information privacy rules became an important goal. The European Commission proposed a Directive in 1990,[211] but the adoption did not conclude until enactment five years later of Directive 95/46/EC. In the intervening years, Europe sought deeper political integration following the ratification of the Maastricht Treaty on European Union.[212] While there is no overt linkage between the political integration of the European Union following the Maastricht Treaty and the final enactment of the data protection directive, the Maastricht Treaty did push European political governance toward greater convergence.[213] Indeed, the European Data Protection Directive

208. *See id.* at 131-35 (examining variations in requirements between European Union Member States).

209. *See Existing Case-Law*, *supra* note 110.

210. *See* REIDENBERG & SCHWARTZ, *supra* note 43, at 139-46.

211. *See* Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, COM(90)314 final.

212. Treaty on European Union, Feb. 7, 1992, 1992 O.J. (C 224) 1 <http://europa.eu.int/eur-lex/en/treaties/dat/eu_cons_treaty_en.pdf>.

213. *See, e.g.*, Armin Von Bogdandy, *The Legal Case for Unity: The European Union as a Single Organization with a Single Legal System*, 36 COMMON MKT. L. REV. 887 (1999) (arguing that the European Union is creating a unitary legal order).

Most jurisdictions, however, have declined to exempt oral contraceptives from the learned intermediary rule.[35] Courts emphasize that, "although a greater degree of patient participation may be involved in the choice of a prescription contraceptive than in some other prescription drugs, the physician makes the ultimate decision as to whether a particular contraceptive requested by the patient is appropriate."[36] The physician still exercises individualized medical judgment. He or she typically "evaluate[s] a patient's medical and family history to elicit potential risk factors, perform[s] a physical examination" and, in cases where a prescription is issued, "determine[s] the appropriate type and dosage to prescribe for a particular patient."[37] Courts also argue that the existence of serious side effects associated with oral contraceptives only underscores the importance of the physician's role in the evaluation of risks and benefits associated with their use.[38] Direct marketing to consumers and the FDA requirements for patient package inserts do not undermine the physician's crucial role in prescribing oral contraceptives.[39] Finally, opponents of the exception argue, "[t]he fact that oral contraceptives do not usually require frequent check-ups bespeaks of the importance of the initial decision to prescribe them and fails to provide a principled basis to depart from the learned intermediary doctrine."[40]

Despite the widespread justification of the learned intermediary doctrine in reproductive health cases, critics of the doctrine have used the rationales supporting the oral contraceptive exception as a springboard for advocating additional exceptions to the rule. The reasoning behind the oral contraceptive exception could arguably be extended to other drugs and medical devices such as those with high risks of side effects;[41] those prescribed elec-

35. *See* MacPherson v. G.D. Searle & Co., 775 F. Supp. 417, 425 (D.D.C. 1991) (applying District of Columbia law); Reaves v. Ortho Pharm. Corp., 765 F. Supp. 1287, 1290-91 (E.D. Mich. 1991) (applying Michigan law); Zanzuri v. G.D. Searle & Co., 748 F. Supp. 1511, 1514-15 (S.D. Fla. 1990) (applying Florida law); Allen v. G.D. Searle & Co., 708 F. Supp. 1142, 1147-48 (D. Or. 1989) (applying Oregon law); Spychala v. G.D. Searle & Co., 705 F. Supp. 1024, 1031-33 (D.N.J. 1988) (applying New Jersey law); Kociemba v. G.D. Searle & Co., 680 F. Supp. 1293, 1305-06 (D. Minn. 1988) (applying Minnesota law); Stafford v. Nipp, 502 So. 2d 702, 704 (Ala. 1987); West v. Searle & Co., 806 S.W.2d 608, 613-14 (Ark. 1991); Lacy v. G.D. Searle & Co., 567 A.2d 398, 400 (Del. 1989); Humes v. Clinton, 792 P.2d 1032, 1040-41 (Kan. 1990); Taurino v. Ellen, 579 A.2d 925, 927 (Pa. Super. Ct. 1990), *appeal denied*, 589 A.2d 693 (Pa. 1991); Terhune v. A.H. Robins Co., 577 P.2d 975, 978-79 (Wash. 1978).

36. *Allen*, 708 F. Supp. at 1148.

37. *Reaves*, 765 F. Supp. at 1290.

38. *See id.* at 1291.

39. For a discussion of direct-to-consumer advertising, see notes 59-80 *infra* and accompanying text. For a discussion of FDA regulations requiring direct warnings, see notes 48-58 *infra* and accompanying text.

40. Walsh, *supra* note 1, at 867.

41. *See* Ferrara v. Berlex Lab., Inc., 732 F. Supp. 552 (E.D. Penn. 1990) (rejecting the argument that the especially dangerous nature of the anti-depressant drug Nardil warranted a direct warning to users).

tively by patients for use over a long period of time;[42] those for which the FDA requires a PPI;[43] and those prescription drugs marketed directly to consumers.[44]

2. *Intrauterine devices and breast implants.*

Relying on the rationales behind the oral contraceptive exception, plaintiffs' attorneys and others have vigorously argued, for instance, that exceptions to the learned intermediary rule also be carved out for intrauterine devices (IUDs) and breast implants.[45] Efforts in this area, however, have met with very limited success. Courts have uniformly declined to impose a direct duty to warn patients in the case of breast implants, and only one court has imposed such a duty in the case of IUDs. Standing alone, the Eighth Circuit in *Hill v. Searle Laboratories*[46] held that the learned intermediary rule should not apply to the IUD for the same reasons other courts had not applied it to oral contraceptives.[47]

3. *FDA regulations requiring direct warnings.*

Some critics of the learned intermediary doctrine advocate an exception to that rule when the FDA has mandated direct patient warnings. Federal regulations promulgated by the FDA currently require manufacturers to supply PPIs for a number of products, including all isoproterenol inhalation preparations, prescription-only contraceptives, estrogens, and progestational drug products.[48] Violation of the federal regulations—by failure to include a

42. Intrauterine devices and breast implants fall under this rubric. For a discussion of efforts to carve out exceptions to the learned intermediary doctrine in this area, see notes 45-47 *infra* and accompanying text.

43. For a discussion of efforts to carve out such an exception to the learned intermediary doctrine, see notes 48-58 *infra* and accompanying text.

44. For a discussion of efforts to carve out a direct-to-consumer advertising exception to the learned intermediary doctrine, see notes 59-80 *infra* and accompanying text.

45. *See, e.g.*, Desmarais v. Dow Corning Corp., 712 F. Supp. 13, 17 n.5 (D. Conn. 1989) (rejecting plaintiff's request to establish a breast implant exception to the learned intermediary rule); Lee v. Baxter Healthcare Corp., 721 F. Supp. 89, 94-95 (D. Md. 1989), *aff'd*, 898 F.2d 146 (4th Cir. 1990) (denying plaintiff recovery under the learned intermediary doctrine in a ruptured breast prosthesis case); Casey, *supra* note 25, at 952-54 (advocating a breast implant exception to the learned intermediary rule). Although not prescription drugs per se, intrauterine devices and breast implants are medical devices, available only through a physician, which illustrate attempts to carve out exceptions to the learned intermediary rule.

46. 884 F.2d 1064 (8th Cir. 1989).

47. *See id.* at 1070-71 (reasoning that birth control decisions are made independently by the patient, thereby reducing the physician's role in making an individualized medical judgment).

48. *See* 21 C.F.R. § 201.305 (1998) (isoproterenol inhalation preparations, used in the treatment of bronchial asthma); *id.* § 310.501(a), (b) (oral contraceptives); *id.* § 310.501a (medroxyprogesterone acetate injectable for contraception); *id.* § 310.502 (intrauterine devices); *id.* § 310.515 (estrogens, hormones used to therapeutically prevent or stop lactation and to improve malignant

November 1997 Ministerial Summit in Turku,[224] the February 1998 workshop on privacy[225] and the Ottawa Summit,[226] the OECD has reasserted its role in data protection, particularly in the context of electronic commerce and online activities. Although the OECD strives to examine data privacy in a cross-sectoral manner,[227] it continues to emphasize the economic perspective on data protection; attention is paid to "users" and "consumers," rather than "citizens." This institutional emphasis draws on the liberal governance model for data protection.

In contrast, from the citizen's rights perspective, the Council of Europe has also begun to address the application of privacy principles to the Internet. In May 1998, the Council of Europe released "Draft Guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highway, which may be incorporated in or annexed to Codes of Conduct," and by February 1999 the Internet guidelines were adopted.[228] Interestingly, the Council of Europe specifically sought to develop these Internet privacy guidelines in conjunction with the European Commission and these guidelines follow a social-protection model. The guidelines reiterate the basic obligations of data collectors and detail the ways in which those collectors should satisfy their data protection obligations.

These institutions clearly want to preserve their relevance and secure an important role in the field of Internet privacy policy. In the Internet context, countries like the United States, with a commitment to liberal governance norms, will clearly support OECD efforts. This does not, however, preclude active participation from countries with social-protection governance norms. To the extent that such countries can influence the results of OECD efforts, points of divergence and conflict may be reduced.

2. *New entrants.*

Despite the reawakening of the OECD and the Council of Europe, these institutions face competition from new entrants to data protection policy that draw heavily on liberal governance norms. The World Trade Organization (WTO), a creation of the Uruguay Round negotiations of the General

224. *See Dismantling the Barriers to Global Electronic Commerce: International Conference*, OECD Doc. No. DSTI/ICCP(98)13/FINAL (Jul. 3, 1998) <http://www.oecd.org/dsti/sti/it/ec/prod/turkufin.pdf>.

225. *See* OECD, PRIVACY PROTECTION IN A GLOBAL NETWORKED SOCIETY: AN OECD INTERNATIONAL WORKSHOP WITH THE SUPPORT OF THE BUSINESS AND INDUSTRY ADVISORY COMMITTEE, OECD DOC. NO. DSTI/ICCP/REG(98)5/FINAL <http://www.oecd.org/dsti/sti/it/secur/prod/reg98-5final.pdf> [hereinafter GLOBAL NETWORKED SOCIETY].

226. *See A Borderless World*, *supra* note 8; *Ministerial Declaration*, *supra* note 68.

227. The OECD Guidelines, for example, apply to all sectors.

228. *See Processing of Personal Data*, *supra* note 68.

Agreement on Tariffs and Trade,[229] will inevitably become involved in data protection and will face privacy issues from the organization's historical commitment to trade liberalization, growth of economic markets, and constraints on state behavior. Indeed, the services provisions of the new trade accords prohibit signatories from imposing restrictions on transborder data flows.[230] While these provisions grant exceptions for privacy-related restrictions, they still preclude each signatory country from taking discriminatory action against other signatories.[231] Consequently, the WTO will have jurisdiction to hear complaints against any national restraint on transborder data flows.[232] The WTO must also initiate studies of issues that affect international trade.[233] Information flows and data protection will clearly be relevant and unavoidable under this mandate.[234] The emphasis will draw on distinctly liberal norms.

The other main intergovernmental entrant is the World Intellectual Property Organization (WIPO).[235] Although the mission of the WIPO is to promote intellectual property protection and rights management, the digital environment merges many intellectual property rights issues with those of data protection. Data protection has implications for the ownership rights to data and the mechanisms for electronic rights management have implications for the fair treatment of personal information.[236] The WIPO cannot ignore the study of data protection as it moves toward the adaptation of intellectual property rights for electronic commerce.

Outside of intergovernmental organizations, technical standards bodies have become stealth entrants. As non-governmental organizations, these groups represent the market forces of liberal norms. These bodies establish technical rules that embed policies for the international flow of personal information. The technical capabilities of new systems have critical ramifica-

229. *See* FINAL ACT EMBODYING THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS: AGREEMENT ESTABLISHING THE WORLD TRADE ORGANIZATION (1994) <http://www.wto.org/wto/eol/e/pdf/04-wto.pdf> [hereinafter AGREEMENT ESTABLISHING THE WORLD TRADE ORGANIZATION].

230. *See* General Agreement on Trade in Services, *in* AGREEMENT ESTABLISHING THE WORLD TRADE ORGANIZATION, *supra* note 229, at Annex 1B, art. XIV(c)(ii) <http://www.wto.org/wto/eol/e/pdf/26-gats.pdf>.

231. *See id.* at art. XIV(c)(ii).

232. For a discussion of possible WTO claims, see Shaffer, *supra* note 129, at 46-55.

233. *See id.* at art. XXIV (creating Council for Trade in Services).

234. In fact, the European Commission has requested consideration of data privacy issues by the Council for Trade in Services. *See* Mario Monti, *The Internet and Privacy: What Regulation* (May 9, 1998) <http://europa.eu.int/comm/internal_market/en/speeches/rome0598.htm>.

235. *See World Intellectual Property Organization* <http://www.wipo.org>.

236. *See* Graham Greenleaf, *'IP, Phone Home' ECMS, ©-Tech, and Protecting Privacy Against Surveillance by Digital Works*, *in* PROC. XXIST INT'L CONF., *supra* note 44; Lee Bygrave & Kamiel Koelman, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems* (June 1998) <http://www.imprimatur.alcs.co.uk/IMP_FTP/privreportdef.pdf>.

tions for data protection. For example, the results of reforms to the domain name system for the Internet may make localization of users and servers easy or impossible. Organizations such as the World Wide Web Consortium (W3C),[237] the Internet Society,[238] the Internet Assigned Numbers Authority (IANA) (now replaced by the Internet Corporation for Assigned Names and Numbers (ICANN)),[239] and the Internet Engineering Task Force (IETF)[240] are each forming data protection policies, though often inadvertently.

These new entrants, in any case, will reflect norms of information privacy from liberal governance rather than social protection. They focus on market development and the allocation of economic interests. The WTO's guiding principle is to increase international trade. The WIPO's mission is to secure intellectual property rights for creators to commercialize their work. And, the prime mission of technical standards bodies, like W3C and IETF, is to promulgate technical standards for market adoption. Nevertheless, proponents of social-protection norms for information privacy have much to gain by working with these new entrants. The constituencies are different from the traditional institutions and the opportunity to find accommodations is valuable.

B. *Technical Codes of Conduct*

These key institutional players reflect a mix of public law-making institutions and rule-setting bodies. The divergence in governance norms, however, assures that attempts to create public law instruments executing First Principles will not satisfactorily resolve data privacy issues for global information networks. International cooperation can, however, focus on technical standards and private solutions as a means to bridge these governance conflicts.

Standards decisions, in effect, mix technical issues with policy choices.[241] The Berlin Group, an organization of national data protection supervisory agencies, has recognized this effect for data protection and identified a set of technical design issues to assure the implementation of First

237. *See* W3C, *About the World Wide Web Consortium* <http://www.w3.org/Consortium/>.

238. *See Internet Society Mission Statement* <http://www.isoc.org/isoc/mission/>.

239. *See The Internet Corporation for Assigned Names and Numbers* <http://www.icann.org/>.

240. For a useful history of these organizations by one of the founders, see Vint Cert, *IETF and ISOC*, July 18, 1995 <http://www.isoc.org/isoc/related/ietf/>.

241. *See* LESSIG, *supra* note 77, at 6 (arguing that technical codes regulate cyberspace); Lorrie Faith Cranor, *The Role of Technology in Self-Regulatory Privacy Schemes, in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997) <http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5B> (discussing the capabilities of technology to provide solutions for privacy protection).

Principles on global networks.[242] In reality, technical choices are "codes of conduct" implementing First Principles just like trade association policy statements seek to define information practices. Technical standards, combined with their deployment and implementation, offer a direct guaranty of fair information practices in any information transfer.[243] These standards operate at the network level and can be independent of national borders. For example, if the infrastructure of an online payment system only allows anonymous transactions, data protection is absolute wherever the transaction takes place on the network.[244] Alternatively, an infrastructure that uses trusted third parties to authenticate and verify the identity of participants in the online payment system may automatically assure fair treatment of personal information by some participants, but not others.[245]

By incorporating data protection within the infrastructure's architecture, technical solutions may specifically be used to arbitrate divergences in national laws.[246] The W3C's "Platform for Privacy Preferences" (P3P)[247] initiative, for example, might one day serve this purpose if server-based filtering can be used to identify and protect against deviations from a juris-

242. These principles are: sensitive data must be encrypted; information and communications technologies must enable users to control and give feedback with regard to his personal data; anonymous access to online services should be available; secure encryption methods must be a legitimate option for Internet users; and quality stamp certification should be explored to improve transparency for users. *See* International Working Group on Data Protection in Telecommunications (IWGDPT), *Report and Guidance on Data Protection and Privacy on the Internet*, Apr. 16, 1996 <http://www.datenschutz-berlin.de/doc/int/iwgdpt/bbmem_en.htm> [hereinafter IWGDPT, *Report and Guidance*].

243. *See* Reidenberg, *Lex Informatica*, *supra* note 78, at 581; *see also* Lessig, *Constitution in Cyberspace*, *supra* note 78, at 898-99 (arguing that technical code is self-enforcing); Reidenberg, *Governing Networks*, *supra* note 78, at 918 (arguing that technical decisions set default rules).

244. *See* Paul F. Syverson, Stuart G. Stubblebine & David M. Goldschlag, *Unlinkable Serial Transactions*, *in* FINANCIAL CRYPTOGRAPHY (Rafael Hirschfed ed., 1997) <http://www.cs.columbia.edu/~stu/97fc.pdf> (proposing alternatives to rectify conflict of interest between service providers and users with respect to personal information).

245. *See, e.g.*, eCash Technologies, *Information for New eCash Issuers* <http://www.ecashtechnologies.com> (allowing for the exchange of ecash payment for goods and services while maintaining security and anonymity for users); David Chaum, *Privacy Technology*, *in* PROC. XVITH INT'L CONF., *supra* note 189.

246. *See* Working Party Established under Art. 29 of Directive 95/46/EC, RECOMMENDATION 1/99 ON INVISIBLE AND AUTOMATIC PROCESSING OF PERSONAL DATA ON THE INTERNET PERFORMED BY SOFTWARE AND HARDWARE, E.C. Doc. No. DG XV 5093/98 WP17 (1999) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp17en.htm> (noting the rule making capacity of software and hardware to support or frustrate European privacy norms); Working Party Established under Art. 29 of Directive 95/46/EC, OPINION 1/98: PLATFORM FOR PRIVACY PREFERENCES (P3P) AND THE OPEN PROFILING STANDARD (OPS), E.C. Doc. No. XV D/5032/98 WP 11 (1998) <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11en.htm> [hereinafter WORKING PARTY, PLATFORM FOR PRIVACY PREFERENCES] (suggesting that technical standards might operate within the European legal framework to assure the protection of privacy in international data flows).

247. *See* W3C, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, Nov. 2, 1999 <http://www.w3.org/TR/1999/WD-P3P-19991102>.

diction's mandatory rules.[248] In particular, P3P might be able to bridge the conflict between the European Union and the United States by assuring "adequate" protection in connection with data flows to the United States. Intelligent agents, as another example, might be used to protect against the secondary use of stored personal information.[249] Agents could be developed to monitor the use of personal information and signal any deviation from specified uses. In either case, such arbitration can maximize international data flows without compromising data protection rules and governance norms.

In this respect, technical arrangements might effectively narrow the scope of divergences in the execution of First Principles. For example, to the extent that technological features make Internet interactions anonymous, data protection issues are minimized or inapplicable. If an Internet protocol address is assigned dynamically so that only the service provider can identify the Web surfer, then a Web site will not know, without more data, who the surfer is. Such features may, however, prove elusive where hidden tools like Web bugs or cookies undercut anonymity. Similarly, to the extent that transparency requirements and registration requirements diverge according to liberal or social protective approaches to First Principles, technological tools might allow the automated satisfaction of different rules for the same transaction. Different notices might be served to users in jurisdictions with specific content requirements and registrations might be automatically generated if data collection occurs in jurisdictions requiring declaration to public authorities. This assumes a circumvention of the Internet's geographic indeterminacy. Likewise, technical restraints analogous to electronic rights-management protocols might be developed to assure finality according to varying obligations. Security protocols can be deployed to prevent all but authorized uses of personal data.

From the perspective of existing data protection regulatory authorities, the treatment of standards as well as their implementation as "codes of conduct" offer a way to avoid governance confrontations. For example, the more recent data protection laws such as the Dutch law and the European Data Protection Directive include procedures for the approval of industry

248. *See* WORKING PARTY, PLATFORM FOR PRIVACY PREFERENCES, *supra* note 246 (noting that European norms need to be incorporated in the technical specifications); *see also* Joel R. Reidenberg, *The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection*, 3 LEX ELECTRONICA (Winter 1997) <http://www.lex-electronica.org/articles/v3-2/reidenbe.html>.

249. *See* International Working Group on Data Protection in Telecommunications, *Common Position on Intelligent Software Agents*, Apr. 29, 1999 <http://www.datenschutz-berlin.de/doc/int/iwgdpt/agent_en.htm>; Netherlands Registratiekamer, *Intelligent Software Agents and Technology: Turning a Privacy Threat Into a Protector* (1999) <http://www.registratiekamer.nl/bis/top_2_5.html>.

codes of conduct.[250] This moves privacy protection to a new forum—the organization preparing the code of conduct. Nevertheless, the forum shift does not vitiate the key role of data protection agencies. Regulators will examine how the codes execute the First Principles and how representative the code will be.[251] If technical codes are included within this purview, then the procedural device can encourage the creation of an infrastructure designed to assure data protection rather than challenge it. Data protection regulators can approve technical codes and implementation configurations like industry policy guidelines. As a consequence, non-European information privacy rules and their national governance norms would lose relevance for Europeans because the technical codes and configurations would assure execution of the First Principles. Through technical standards, international data flows can respect diverging governance norms through automated compliance rules that satisfy obligations in both the home and host countries. Significantly, multiple technical standards can coexist for information flows in cyberspace.[252] Hence, one standard that might satisfy the disclosure requirements in a given country does not preclude simultaneous use of another standard that assures finality in a different country. The biggest obstacles will be the time necessary to reach agreement on a code and the take-it or leave-it choice that some companies may find difficult.

C. *Multistakeholder Summits*

Although technical codes of conduct can minimize the conflict among divergent information privacy norms, the dynamic nature of information processing in the online environment means that national governments must have an ongoing dialog with all stakeholders, including industry and privacy advocacy groups as well as independent experts and scholars. Such an open dialog is crucial to the future of international data flows and the development of coherent policies.

The OECD Workshop on Privacy in February 1998[253] and the White House conference on privacy in June 1998[254] are useful models for this form

250. *See European Data Protection Directive*, *supra* note 11, at art. 30(1) (d).

251. *See* Working Party Established under Art. 29 of Directive 95/46/EC, FUTURE WORK ON CODES OF CONDUCT: WORKING DOCUMENT ON THE PROCEDURES FOR THE CONSIDERATION BY THE WORKING PARTY OF COMMUNITY CODES OF CONDUCT, E.C. Doc. DG XII D/5004/98 WP13 (1998) <http://europa.eu.int/comm/internal_market/media/dataprot/wpdocs/wp13en.htm>.

252. This conceptual insight underlies the W3C movement for P3P. The technical protocol for P3P allows multiple privacy ratings and filtering to coexist.

253. *See generally* GLOBAL NETWORKED SOCIETY, *supra* note 225.

254. *See generally* U.S. DEP'T OF COMMERCE, *Public Meeting*, *supra* note 219. The meeting was designed as a forum to discuss issues for the Commerce Department and the Office of Management and Budget (OMB) report to the President on self-regulation and Internet privacy. *See* National Telecomm. and Info. Admin., U.S. Dep't of Comm., Elements of Effective Self Regula-

of multi-interest summitry. Though few substantive advances were achieved, dialog and information sharing occurred among the private sector, academic experts, advocates, and government. The business lobby is increasingly seeking to synthesize data protection into a notice and consent framework, so this type of multistakeholder approach helps preserve consensus on the First Principles and may lead to greater governance convergence for implementation.

At the international level, the OECD is a logical organization to convene such conferences. The OECD has experience in fostering dialog between government and business.[255] More recently, however, the OECD has been quite sympathetic to business and less directly concerned with citizen's rights. For example, the Business and Industry Advisory Committee is a nonvoting, accredited observer,[256] but no privacy organizations have such official observer status.[257] Although many country delegations to the OECD contain representation from national data protection regulators, the U.S. delegation does not, and it typically plays a significant role at intergovernmental meetings, stressing the liberal, market approach. The success of future summits will, thus, depend on the balance achieved between the airing of business views and the critiques of those without commercial interests at stake.

For the OECD to continue to proceed effectively, it must seek the participation of each of the interest groups. Accreditation for privacy organizations and the formation of a standing expert advisory committee will be necessary. Such multi-interest summits should occur on a biennial basis to assure sufficient frequency and high-level participation.

D. *General Agreement on Information Privacy*

While technical codes and international summitry may facilitate the coexistence of divergent executions of First Principles, fundamental differences are likely to persist in areas where governance norms force a clash of public order.[258] When, for example, data privacy violations have criminal sanctions, divergences may be hard to coregulate. The treatment of sensitive data presents such a case. Where consent is rejected as a basis for processing

---

tion for the Protection of Privacy and Questions Related to Online Privacy, June 5, 1998 <http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm>.

255. For example, the OECD consults regularly with the Business and Industry Advisory Committee, an international consortium of trade associations. *See OECD and the Public* <http://www.oecd.org/about/public/index.htm>.

256. *See About BIAC* <http://www.biac.org/biac.htm>.

257. The Trans Atlantic Consumer Dialogue, a consortium of national consumer groups, is also an observer to the OECD, but is not expressly a privacy organization.

258. *See* Goldsmith, *supra* note 114, at 1210 (discussing the relative ease of resolving conflicts between default rules as compared with mandatory laws).

certain forms of personal information,[259] such as medical information, technical rules based on consent cannot function to arbitrate among divergent national laws.

The time has come, therefore, for a new type of international treaty on data protection.[260] At the 1997 International Privacy Conference in Montreal, the Quebec organizers proposed the creation of a new international privacy organization, an international privacy secretariat.[261] The goal was to move toward a more coordinated international response to information privacy divergence. The real problem, however, is not lack of convergence on First Principles, but instead the lack of harmonization on democratic governance norms for information privacy.

Rather than the establishment of an international privacy secretariat composed of interested participants, data protection needs an intergovernmental "General Agreement on Information Privacy" (GAIP) that includes a large number and wide range of signatory countries. GAIP should focus on establishing an institutional process of norm development designed to facilitate in the near term the coexistence of differing regimes, and over time promote harmonization of governing standards for information privacy.

The GATT compromise in 1947 offers a useful model for this first step toward effective international cooperation. After the failure of the Havana Charter to create an International Trade Organization, the resulting GATT was as important originally for the establishment of an institutional mechanism that allowed countries to address trade disputes as it was for the substantive reductions in tariffs and quotas.[262] Like the GATT concept in 1947, the GAIP treaty should recognize basic principles of data protection and create a high-level negotiating forum for consensus-based decisions. By institutionalizing such negotiations in a multilateral setting, two important data protection objectives may be achieved. First, counterparts for data protection policy discussions will be clearly designated even in countries without ex-

259. *See* Mayer-Schonberger, *supra* note 2, at 233 (discussing various European laws imposing forms of mandatory legal protection).

260. Although the Council of Europe Convention has had some success as an international treaty on data protection, the instrument lacks a sufficiently broad range of signatories and has not achieved the degree of harmonization necessary for information flows in the online world to function effectively. Twenty countries have ratified the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. *See Chart of Signatures and Ratifications*, Feb. 11, 1999 <http://www.coe.fr/tablconv/108t.htm>. Most notable among the signatory absences is the United States. Since the United States is unlikely to agree in the near term to an obligatory set of data protection principles as a result of its liberal, market approach, the Council of Europe Convention will not be able to expand effectively.

261. *See* Raymond Doray, *A Word From the President of the Conference*, *in* PRIVACY: THE NEW FRONTIER, PROGRAM BOOK OF ABSTRACTS FROM THE INTERNATIONAL CONFERENCE ON PRIVACY 5 (Sept. 1997).

262. *See* WTO, *Roots: from Havana to Marrakesh* <http://www.wto.org/wto/about/facts4.htm#GATT>.

isting data protection authorities. This applies specifically to the United States where data privacy issues rotate almost indiscriminately among different government agencies depending on the interests of particular people at the agencies.[263] Second, expansive representation and regular negotiations can predictably lead to increased consensus over time on necessary standards. The GATT evolution toward the Uruguay Round accords and the adoption of the GATT 1994 illustrate this latter trend. Between 1948 and 1994, GATT was tremendously successful in liberalizing world trade and including new concepts such as intellectual property and services within the global mercantile system.[264] Moreover, the diversity of countries represented in GATT afforded developing countries and less-powerful countries a better chance to influence trade issues in the multilateral framework than they would have had on a bilateral basis.[265] The resulting accords would have stronger consensus around the world.

Beyond a mere model, the World Trade Organization (WTO), successor to the GATT, offers a useful launching point for the GAIP. The WTO has an institutional mechanism to study and negotiate new trade issues. Every two years, WTO members must convene a ministerial-level conference to review and examine world trade, including trade in global services.[266] Although pursuing a WTO strategy places data protection in the trade arena rather than a political arena, WTO increasingly faces the incorporation noneconomic values in trade policy.[267] The risk of placing GAIP within the WTO trade framework is that the WTO has an inherent bias toward liberal, market norms; GATT and the WTO are founded on the principle of free trade and market economies.[268] The typical remedies for a violation of WTO principles are trade sanctions rather than private damages or injunctions to vindicate personal rights. Nonetheless, the breadth of membership in WTO and the growing recognition at WTO that social values such as workers' rights and environmental issues are intrinsically linked to trade will blend govern-

263. *See* Gellman, *supra* note 53, at 237 (describing the agencies that have had general or international privacy policy responsibilities).

264. *See* WTO, *Roots: from Havana to Marrakesh*, *supra* note 262.

265. *See id.* at 5 ("Developing countries and other less powerful participants have a greater chance of influencing the multilateral system in a trade round than in bilateral relationships with major trading nations.").

266. *See* AGREEMENT ESTABLISHING THE WORLD TRADE ORGANIZATION, *supra* note 229, at art. IV; WTO, *The Trade Policy Review Mechanism* <http://www.wto.org/wto/reviews/tprm.htm> (explaining the regular review process for signatory countries that includes services).

267. Environmental and labor/workers rights issues were topics of discussion at the Seattle Ministerial Conference. *See* WTO, *Seattle: What's at Stake? Concerns . . . And Responses* <http://www.wto.org/wto/minist1/stak_e_6.htm>. Despite the protests and controversy surrounding the Seattle Ministerial Conference, these social issues remain at the forefront of international trade discussions.

268. *See* SWIRE & LITAN, *supra* note 10, at 195-96 (discussing the WTO as a forum for negotiating privacy concerns).

ance ideologies.[269] Noneconomic values will bring non-market based governance norms to WTO. This is likely to happen with or without GAIP negotiations in a WTO context. Indeed, in the context of information flows, this transformation has already begun. The WTO accords expressly recognize privacy as a value that can override the free flow of information principle enshrined in the annex agreement on services.[270] The significance of putting GAIP before the WTO is, thus, twofold. First, the WTO framework offers an institutional process with wide membership. Second, while the institution leans toward market-based norms, the incorporation of GAIP within the WTO along with other noneconomic values will transplant social-protection norms to the trade arena. In effect, this transplantation will promote convergence of governance norms.

VI. STRATEGIES FOR CO-ORDINATION AND COOPERATION

For transplantation and convergence to occur in the context of First Principles, a map of strategies and partners is needed to inform and promote coregulation and eventual consensus on the governance issues related to the protection of personal information in data transfers. Since the release of the proposal for the European Data Protection Directive in 1990, Europe has shaped the debate and agenda for international privacy issues.[271] Strategies and alliances must, therefore, start with the international political dimensions of Internet data flows. Moreover, Europe has well-established and active national regulatory agencies for data protection. These data protection commissions are, thus, at the heart of the movement building a deeper consensus on the integration of First Principles in different countries.

A. *Political Dimensions*

The political dimensions are at a critical stage for international data flows. The European Union has taken a strong rhetorical position in favor of the examination of foreign data protection rules and in support of embargoes

269. *See* WTO, *Director-General's Message: Seattle Ministerial Conference Must Deliver for the Poorest, Says Moore* <http://www.wto.org/wto/minist1/02dg_e.htm> (quoting WTO Director-General Michael Moore noting the importance of considering environmental and labor issues in the next trade negotiating round).

270. *See* General Agreement on Trade in Services, *supra* note 230, at annex 1B, art. XIV(c)(ii).

271. *See, e.g.*, Bennett, *supra* note 2, at 108-14 (describing the impact of the European Data Protection Directive on the policies of states that have not passed similar measures); Priscilla M. Regan, *American Business and the European Data Protection Directive: Lobbying Strategies and Tactics*, *in* VISIONS OF PRIVACY, *supra* note 51, at 199, 200-01 (describing the reaction of U.S. industry to the European Data Protection Directive); Samuelson, *supra* note 76, at 751-52 (describing the reasons why American lawyers will have to become familiar with the emerging body of information privacy law).

of data going to destinations with inadequate levels of protection.[272] But, the European Union faces many challenges to the strict enforcement of these rules. The Member States are likely to have different views on particular cases, and Europe does not appear to seek an impenetrable data fortress.[273]

Internal or national political realities also have consequences for international data flows. Within Europe, for example, the transposition of the European Data Protection Directive into Member State law illustrates the political fluidity of data protection.[274] Bureaucratic squabbles and political maneuvering will determine the specific outcomes of transposition and will set the tone for each country's international posture.[275] Outside of Europe, these "turf" battles will be particularly acute in countries without data protection authorities, like the United States. Where there is no existing data protection authority, differing government agencies are likely to fight over jurisdiction and hence power.[276] Compromises are likely to result in a series of agencies having pieces of responsibility for data protection policy. In addition, as seen in the United States, industry lobbyists are likely to promote agencies such as the U.S. Department of Commerce, which are traditionally more

272. *See European Data Protection Directive*, *supra* note 11, at art. 25; Brühann, *supra* note 120.

273. *See, e.g.*, Letter from Fred H. Cate, Robert E. Litan, Joel R. Reidenberg, Paul M. Schwartz & Peter P. Swire to the Ambassador David L. Aaron, Undersecretary for International Trade, U.S. Dep't of Commerce (Nov. 17, 1998) <http://www.acs.ohio-state.edu/units/law/swire1/DOCCOMME.htm> (noting that the U.S. Commerce Department's Draft International Safe Harbor Privacy Principles, although designed to comply with EU data privacy policy, fails to meet E.U. data privacy standards on several important points).

274. As of July 1999, nine Member States (France, Luxembourg, the Netherlands, Germany, the United Kingdom, Ireland, Denmark, Spain, and Austria) had failed to transpose the Directive into national law and received a formal warning from the European Commission. *See* European Commission, *Data protection: Commission Decides to Send Reasoned Opinions to Nine Member States*, July 29, 1999 <http://europa.eu.int/comm/dg15/en/media/dataprot/news/99-592.htm>.

275. In France, for example, the Braibant Report issued in March of 1998 on the transposition of the European Directive into French law has led to various public discussions. *See* Données personnelles et societé de l'information: Rapport au Premier Ministre sur la transposition en droit français de la directive no. 95/46, Mar. 3, 1998 <http://www.premier-ministre.gouv.fr/PM/RAPPORTS1.HTM#1> (linking to the Braibant Report). But, there is still no bill before the Parliament. *See* Ministry of Economy, Finance, and Industry, *Policy Paper on the Adaptation of the Legal Framework [sic] the Information Society*, at § 1.6 (Oct. 1999) <http://www.finances.gouv.fr/societe_information/anglais/chapitre1_ang.htm>.

276. In the United States, there is a musical chairs approach to agency responsibility for information privacy policy. *See, e.g.*, Gellman, *supra* note 53. Interest has rotated among the OMB, NTIA, USTR, FCC, FTC, the State Department, and the Commerce Department. At the moment, the FTC seems to be taking the lead on privacy issues. In 1998, the Clinton Administration established an office within the bureaucratic layers of the OMB and Professor Swire was appointed to the post. *See* Declan McCullagh & James Glave, *Clinton Tabs Privacy Point Man*, WIRED NEWS, Mar. 3, 1999 <http://www.wired.com/news/news/politics/story/18249.html>. The position does not, however, have policymaking authority and Professor Swire's precise role in privacy issues remains unclear. *See* Shaffer, *supra* note 129, at 62-63.

sympathetic to the interests of industry than of individuals.[277] These political alignments will complicate efforts for international cooperation.

Yet, despite the political flux, each of the European Union Member States has an existing data protection agency. These regulators will seek to define their institutional place in the further development of international norms. Since they form an important elite community of policymakers,[278] they will strive for an active role.

B. *Roles of Data Protection Commissions*

As the instruments and institutions affecting international data flows and the protection of personal information evolve, data protection authorities will have a vital role in the resolution of international conflicts. Data protection authorities can act as emissaries for fair information practices, but also serve as advocates for the rights of individuals in the tradition of their socially-protective governance norms. These two key strategies and their corresponding partners offer data protection authorities a powerful means to promote convergence on socially-protective norms for international data flows.

1. *Emissary strategy.*

The emissary strategy consists of representing the socially-protective approach in a variety of international contexts. By exposing and highlighting fair information practice standards with different governmental and nongovernmental partners at the international level, data protection authorities can reduce misunderstandings, find ways to enable the peaceful coexistence of national data protection approaches, and move toward consensus on execution of First Principles. Three types of partners are critical to this endeavor: data protection authorities themselves, foreign governments, and international organizations.

International cooperation among data protection authorities is well established on both formal and informal levels. The annual Commissioners' meeting,[279] the regular meetings of the International Working Group on Data Protection in Telecommunications (the Berlin Group),[280] and the quarterly

277. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 78 (1995) (noting the early opposition to privacy regulation by the U.S. Department of Commerce).

278. *See* BENNETT, *supra* note 10, at 127-29 (describing how these policymakers separately lobby their governments to effect change).

279. *See, e.g.*, PROC. XXI INT'L CONF., *supra* note 44.

280. The International Working Group on Data Protection in Telecommunications was established by the Berlin Data Privacy Commissioner. For information about their activities, see *International Working Group on Data Protection in Telecommunications* <http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm>.

sessions of European commissioners under the auspices of the Article 29 Working Party[281] each reflect organized efforts to promote shared data protection interests among national authorities. More informally, direct contacts among Commissioners and discussions at prominent international conferences such as the annual conference organized by Privacy Laws & Business at the University of Cambridge[282] also serve an important role in coordinating resources and expertise.

Yet, these emissary contacts should move to the next stage and exploit new opportunities to promote international consensus. Emissaries can take collective policy positions that advance the understanding of fair information practices for international data flows. The Berlin Group and the Article 29 Working Party have begun to issue such declarations and interpretations of data protection principles.[283] These documents help set and define the international agenda. Future Data Protection Commissioners' Conferences should issue final substantive declarations at the conclusion of the Commissioners' annual private session.[284] Such a strategy would focus preparatory work by the host Commission and promote consensus among the data protection authorities. Over time, such declarations would build a strong and clear set of standards for the execution of First Principles in the context of international data flows.

However, since many countries around the world, including the United States, do not have a national data protection agency, contacts between data protection authorities and foreign governments must also be developed. A number of data protection authorities have pursued this strategy with the United States as has the European Commission.[285] The strategy is a complicated one because foreign government counterparts may not be stable. In the United States, for example, each year seems to find a different government agency in charge of the domestic privacy agenda. As many at the Commissioners' conference have noted, when the U.S. government sends observers

281. *See European Data Protection Directive, supra* note 11, at art. 29.

282. *See* Privacy Laws & Business, *Conferences* <http://www.privacylaws.co.uk/conferences.htm>.

283. *See International Working Group on Data Protection in Telecommunications, supra* note 280, at 1 (listing declarations of the Berlin Group and links to texts); European Comm., *Documents Adopted by the Data Protection Working Party* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm>.

284. *See* Joel R. Reidenberg, *International Data transfers and methods to strengthen international cooperation, in* PROC. XXTH INT'L CONF. DATA PROT. COMM'RS (1998) <http://home.sprynet.com/~reidenberg/idt.htm> (arguing for a final conference declaration); *Declaration on Privacy and the Internet of the European Privacy Commissioners and Iceland, Norway and Switzerland* <http://www.cnil.fr/actu/communic/actu6.htm> (common position taken at the conclusion of the conference by many of the commissioners).

285. In particular, negotiations are underway between the European Commission and the U.S. Department of Commerce to try to find a "safeharbor" policy for the U.S. to qualify for international data transfers under the European Directive. *See* Letter from Ambassador David L. Aaron to Colleagues (Nov. 15, 1999) <http://www.ita.doc.gov/td/ecom/aaronmemo1199.htm>.

to the annual meeting, there is little continuity in either the staff or the U.S. government agency being represented.[286]

Since several different government offices in many countries may have jurisdiction over data protection matters, data protection authorities risk being caught in the internal disputes of foreign government bureaucracies. This makes emissary contacts more elusive, but no less critical. If a country's internal data protection policy apparatus is not stable, the potential for international conflicts multiplies. Data protection authorities will need to seek the assistance of their own government offices to sort out some of the diplomatic issues and identify the key domestic policy players.

As the traditional institutions of data protection (the OECD and the Council of Europe) seek to expand their role in international conflict resolution and as the new entrants (the WTO and the WIPO) begin to address fair information practice issues,[287] data protection authorities can offer valuable expertise and insight, while ensuring that their perspectives are not lost. This will be a particularly critical role since the new entrants tend to approach data protection from the perspective of liberal governance norms. The emissary strategy with international organizations will, in essence, help frame these organizations' agendas for international cooperation.

Nevertheless, the avenues for input at most of these organizations are not familiar to data protection authorities. For the OECD, the WTO, and the WIPO, it is typically commerce departments or finance or economic ministries that coordinate national participation. Data protection authorities will need to vigilantly participate on country delegations to these fora. In contrast, at the Council of Europe, foreign affairs ministries are more active and data protection authorities have had regular channels of participation. These must continue.

2. *Advocacy strategy.*

In addition to the emissary strategy, data protection agencies should pursue an advocacy strategy that involves the active promotion of specific execution standards of First Principles. Paradoxically for international cooperation, this strategy may be confrontational at times. Confrontation can facilitate ascertaining whether differences on issues are slight or fundamental. Where the differences are fundamental, advocacy may force compromises and solutions. This advocacy strategy for data protection agencies applies to three types of counterparts: foreign governments, technical or-

286. For example, at the 1992 Commissioners' Conference, a representative from the State Department attended as the U.S. observer; at the 1998 conference, the United States sent a representative from the NTIA (an agency of the U.S. Department of Commerce) and at the 1999 conference, a representative from the OMB participated.

287. *See* text accompanying notes 229-236 *supra.*

ganizations, and foreign organizations (e.g., companies and trade associations).

The advocacy strategy is clearly in progress between the United States and Europe over the implementation of Articles 25 and 26 of the European Data Protection Directive and its equivalents in national laws.[288] Since the start of the process to adopt the European Data Protection Directive, the international agenda on specific data protection standards has largely been set by the European Union and several of the Member State data protection authorities. By setting a minimum threshold of protection as a condition for data exports from Europe, the Directive along with the prior law in several of the Member States embodies a strong position against data havens and a potentially confrontational position with respect to non-European Union governments.

In response, the American position for the past eight years has been largely defensive. At first, the U.S. government firmly asserted that American data protection was equal to that in Europe. Europeans had access to unfiltered sources of information about the U.S. system and were not persuaded.[289] Continued European advocacy pushed the U.S. government to try to justify reliance on self-regulation. This example illustrates that the confrontational risk of transborder data flow restrictions has worked as an effective negotiating tool and that the agenda-setting function is a particularly valuable aspect of the advocacy strategy.

The advocacy strategy is particularly important to influence the work occurring in technical organizations such as W3C, the International Organization for Standards (ISO), the Internet Society (ISOC), and IANA. Too often, data protection authorities ignore technical discussions. While the Berlin Group took an important step by becoming involved in consultations with W3C over a privacy transmission protocol, this input appears more in an ad-

288. Since November 1998, the U.S. Department of Commerce and the Directorate General XV of the European Commission have been negotiating the evaluation of U.S. data privacy under the "adequacy" criteria of Art. 25 of the European Directive. The Working Party established under Article 29 of the European Directive, which is composed of representatives from each of the national regulatory authorities, has insisted on strong protections from the U.S. side. *See* Working Party Established Under Art. 29 of Directive 95/46/EC, *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government*, E.C. Doc. DG XV 5092/98 WP 15 (Jan. 26, 1999) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp15en.htm>; Working Party Established Under Art. 29 of Directive 95/46/EC, *Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" Issued by the U.S. Department of Commerce on 19th April 1999*, E.C. Doc. DG XV 5047/99 WP 19 (May 3, 1999) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp19en.htm>; Working Party Established Under Art. 29 of Directive 95/46/EC, *Opinion 4/99 on the Frequently Asked Questions to Be Issued by the U.S. Department of Commerce in Relation to the Proposed "Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles,"* E.C. Doc. DG XV 5066/99 WP 21 (June 7, 1999) <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp21en.htm>.

289. *See* Spiros Simitis, *Foreword*, *in* SCHWARTZ & REIDENBERG, *supra* note 9, at viii-ix.

visory role than an advocacy role.[290] As advocates, data protection authorities can insist on certain standards or technical capabilities as a prerequisite to the permissible use of the technology for processing personal information.[291] France, for example, used this approach with the providers of software for airline reservation systems and incorporated this strategy in the 1996 Telecommunications Law that imposes liability on service providers who fail to offer content filtering capabilities to their Internet service subscribers.[292]

Nonetheless, the Berlin Group's involvement in technical fora seems exceptional. Such involvement is not a priority of many data protection authorities. For example, the data protection authorities were hardly involved while the structure of the Internet domain name system was reorganized.[293] These policy debates in technical areas offered a significant opportunity to build specific data protection options into the architecture of the Internet. The name system could be structured to both assure anonymity of personal information and to enable the application of data protection principles to online activities. In other areas of technical standardization there are significant opportunities to make anonymous use of the Internet more accessible or to establish data protection icons, like a logo, that might reflect particular substantive rules, policies, and practices. Similarly, technical standards that enable automation devices to bridge differences across data protection rules could be developed. For example, protocols might be used to automate compliance with different notice requirements such as prerequisite disclosures and different consent mechanisms.

One of the explanations for the hesitance of data protection authorities in the technical arena is that this advocacy strategy changes the personnel dynamic within data protection agencies. Agency staff need greater technical expertise. In particular, staffers must be as comfortable speaking of "meta-

290. *See* Internet Working Group on Data Protection in Telecommunications, *Common Position on Essentials for Privacy-Enhancing Technologies (e.g. P3P) on the WorldWideWeb* (Apr. 15, 1998) <http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm> (setting forth broad objectives that any privacy protocol should meet).

291. *See, e.g.*, IWGDPT, *Report and Guidance*, *supra* note 242, at ¶ 4 ("In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law.").

292. Law No. 96-659 of July 26, 1996, art. 15, J.O., July 27, 1996, p. 11384, 11395.

293. As ICANN and the WIPO have outlined rules for the collection and dissemination of domain name registry information, data protection commissioners have remained silent. Professor Michael Froomkin, as the "public interest representative" to a panel of experts convened by the WIPO, singlehandedly brought the privacy issue onto the table in his stinging critique of the early draft of the WIPO guidance. *See* A. Michael Froomkin, *A Critique of WIPO's RFC3 Ver. 1.0a* (Mar. 14, 1999) <http://www.law.miami.edu/~amf/critique.htm> (describing initial proposals as "zero privacy"); WIPO, *Panel of Experts* <http://ecommerce.wipo.int/domains/process/eng/experts.html) (listing Prof. Froomkin as consulted expert).

tags" as they are thinking about "purpose specifications." This shift is necessary, but likely to be difficult for some agencies.

In any case, without a strong advocacy strategy from data protection authorities, technical organizations and their clients are unlikely to implement standards in a manner that actively promotes basic principles of data protection. W3C provides a useful illustration of the resistance. The technology for filtering Internet content as well as privacy practices has been available for almost four years.[294] The Platform for Internet Content Selection (PICS) began at W3C as a response to Congressional interest in prohibiting children's access to offensive material on the Internet and was developed as a transmission protocol to enable content labeling and filtering. The same technology can be applied to match Web site privacy policies with visitor privacy preferences; W3C began to develop this application, Platform for Privacy Preferences (P3P), in 1996. Yet, to date, neither PICS nor P3P have settled standards and wide-spread acceptance. And, the P3P effort is essentially a U.S.-led exercise. In the absence of an advocacy strategy with a few confrontations, the incentive structure does not exist for the technical organizations to focus on the international dimensions of national standards and companies have little real incentive to implement privacy technologies that adequately secure citizens' rights.

In many countries without data protection agencies, like the United States, the advocacy strategy plays a critical role in persuading foreign organizations to adopt standards of fair information practice. Communications from data protection authorities to foreign organizations such as companies or trade associations fill the gaps where data protection authorities have no counterpart. The effectiveness of this strategy is demonstrated by the European Commission's dialog with U.S. business groups. Many U.S. industries and companies have developed data protection programs during the last several years largely in response to the perceived threat from the European Data Protection Directive.[295]

The expansion of direct advocacy to foreign organizations offers a means for data protection authorities to assure execution of First Principles for international data flows. As advocates, data protection officials can use confrontations over transborder data flow prohibitions to find solutions such as contracts stipulating liability of exporters like the Citibank/Bahncard exam-

294. FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (June 4, 1996) <http://www.ftc.gov/bcp/privacy/wkshp96/pw960604.pdf> (statement of Paul Resnick, AT&T Research) (describing the possibility of adapting PICS for information privacy protection).

295. *See, e.g.*, Trans Atlantic Business Dialogue, *Statement of Conclusions* (1999) <http://www.tabd.org/recom/berlin.html> (discussing industry protection of personal data for e-commerce); U.S. Council for International Business, *Privacy Diagnostic* (1998) <http://www.uscib.org/policy/privmin.htm> (offering tool for companies to develop privacy policies that facilitate transborder data flows).

ple in Germany.[296] In the long term, direct advocacy to foreign organizations is likely to lead to increased participation by the governments of those countries and an increasing centralization of data protection policy in those countries. This will, in turn, promote the establishment of a counterpart for discussions with existing foreign data protection authorities. This is starting to occur in the United States. With the emphasis from Europe on international data protection, the Clinton administration created a Chief Counselor for Privacy in the OMB.[297] Ironically, the practical effect returns the focus to the convergence of governance norms: Centralization of data privacy policy is anchored in socially-protective norms rather than liberal, market norms. Thus, the advocacy strategy promotes international convergence of governance norms for the protection of information privacy.

CONCLUSION

This article makes a number of claims about the nature of information privacy rules and their variation across borders. First, the article claims that a global convergence exists in democracies on First Principles, a core set of standards for fair information practice. But, divergence in the execution of those principles both in approach to law and interpretation of law remains significant. Second, the article argues that the nature of these divergences runs much deeper than differences in legal systems and goes to the core norms of a democratic society's organization regarding choices about the role of the state, market, and citizen in society. Liberal, market norms of democratic organization lead to different expressions of information privacy rules than socially-protective norms.

International data flows on the Internet force these divergent rules to confront each other with increasing frequency. The claim that divergences draw on different governance norms means that privacy conflicts will only be resolved by finding compatibility points or by convergence of those very governance norms. Starting with a search for compatibility, the article develops a theory for coregulation and highlights both strategies and methods for data protection authorities to promote international data flows through multinational coordination and cooperation. None of the instruments and strategies are mutually exclusive. To the contrary, they collectively form an important basis to strengthen international convergence on the execution of First Principles. Indeed, these are methods to steer privacy.[298] Paradoxi-

296. *See* Dix, *supra* note 4 (describing the requirement of the Berlin Privacy Commission for Citibank to execute a data privacy contract with its German affiliate prior to the transfer of credit card data to the United States).

297. *See* James Glave, *Privacy's Protector Makes Debut*, WIRED NEWS, Mar. 5, 1999 <http://www.wired.com/news/politics/0,1283,18301,00.html>.

298. Charles D. Raab, *From Balancing to Steering: New Directions for Data Protection*, *in* VISIONS OF PRIVACY, *supra* note 51, at 83-88.

cally, if coregulation facilitates information privacy on global networks, then the increasing and successful contact between different systems should lead to legal transplantation—the incorporation by one legal system of rules developed in another system.[299] In effect, this will become a force of convergence for governance norms. To the extent that countries adopt information privacy mechanisms from other democracies, they will also be adopting philosophies about the role of states, citizens, and markets in society. In the long term, privacy issues may turn out to drive a global convergence on governance norms for the Information Society.

299. *See* Alan Watson, *Aspects of Reception of Law*, 44 AM. J. COMP. L. 335, 335 (1996) (discussing four forces affecting legal transplants: (1) extreme practical utility; (2) chance; (3) difficulty of clear sight; and (4) the need for authority).

* * *