Book Review

A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy

DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION. By Paul M. Schwartz† & Joel R. Reidenberg.†† Charlottesville: Michie, 1996. Pp. xxiv, 486. $90.00.

NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE. By Peter P. Swire††† & Robert E. Litan.†††† Washington, D.C.: Brookings Institution Press, 1998. Pp. 269. $24.95.

Reviewed by Pamela Samuelson†††††

INTRODUCTION

Two reasons explain why American lawyers of the next decade will need to become familiar with a newly emerging body of information privacy law. The first arises from the European Union's adoption of a complex regulatory regime that mandates strict legal protection of personal information about European citizens[1] stored or processed by virtually all private and certain public sector entities.[2] To ensure that offshore data havens cannot undermine its regulatory regime, the European Council's Directive outlaws transborder flows of personally identifiable data between the Enropean Union (E.U.) and any jurisdiction having "inadequate"

† Professor of Law, Brooklyn Law School.

†† Professor of Law, Fordham Law School.

††† Professor of Law, Ohio State University College of Law.

†††† Director of the Economics Studies Program and holder of the Cabot Family Chair at the Brookings Institution.

††††† Professor of Law and of Information Management, University of California, Berkeley.

1. *See* Council Directive 95/46, 1995 O.J. (L281) [hereinafter Directive]. The Directive is reprinted in PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE app. A at 213 (1998). The principal purpose of the Directive is to harmonize the disparate data protection laws of the European Union's member states. *See id.* at 23.

2. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 1 (1996).

standards of data protection.[3] E.U. officials have made no secret of the fact that they regard the U.S. approach to data protection as generally inadequate,[4] and U.S. and E.U. officials have been negotiating for some time—with little success, it should be said—to find an amicable resolution of their differences on data protection issues.[5] In the meantime, however, U.S. firms have reason to worry that their transborder data flows with European branches, customers, suppliers, or consultants might run afoul of the European Union's complex new rules, making U.S. firms vulnerable to litigation, fines, or a disruption of the data flows on which they may depend.[6]

The second reason why American lawyers will need to become familiar with information privacy law arises from the American populace's emergent awareness of, and concern with, the widespread use of information technologies—particularly those connected to digital networks—to build profiles of individuals.[7] Information technologies can amass, cross-correlate, and process extraordinary volumes of information, both trivial and important, sensitive and not so sensitive, about the minutiae of individuals' activities and preferences.[8] The so-called "Bork law," which outlaws revealing information about videotape rentals by specific individuals,[9] illustrates that the American public can be mobilized to support legislation to enforce "fair information practices."[10] As the American public becomes more conscious both of the ubiquity of automated personal data collection by private and public sector entities and of the multiple unauthorized uses of that data, demand may grow for more legislation to prevent abuse.[11] American lawyers will need to be familiar with such legislation.

The idea of legal protection for personal data resonates so little with the average American lawyer today that it is surely not easy to decide what

---

3. *See* Directive, *supra* note 1, arts. 25-26.

4. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 206-07; SWIRE & LITAN, *supra* note 1, at 2-3.

5. *See* Joe Kirwin & Gary Yerkey, *E.U. Rejects U.S. Data Privacy Plan; Next Round of Talks Set for Dec. 1*, Electronic Com. & L. Rep. (BNA) No. 45, at 1337 (Nov. 25, 1998).

6. *See* SWIRE & LITAN, *supra* note 1, at 42-48.

7. *See id.* at 80 (citing polls).

8. Some scholars observe that heightened surveillance seems to be an inherent part of the modern information society. *See, e.g.*, ANTHONY GIDDENS, MODERNITY AND SELF-IDENTITY: SELF AND SOCIETY IN THE LATE MODERN AGE (1991); 2 ANTHONY GIDDENS, THE NATION-STATE AND VIOLENCE (1985).

9. Video Privacy Act, 18 U.S.C. §§ 2710-2711 (1994), *discussed in* SCHWARTZ & REIDENBERG, *supra* note 2, at 10-11.

10. SCHWARTZ & REIDENBERG, *supra* note 2, at 10.

11. After the Federal Trade Commission hearings revealed abuses in the collection of information from children, the U.S. Congress passed new legislation forbidding firms from collecting data from children under the age of thirteen. *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681; *see also* U.S. GOV'T WORKING GROUP ON ELEC. COMMERCE, FIRST ANNUAL REPORT (Nov. 1998) [hereinafter ELECTRONIC COMMERCE FIRST ANNUAL REPORT] (discussing this hearing and the subsequently passed Children's Online Privacy Protection Act).

title to give to a U.S.-published book on this subject, let alone how to market the book. A European audience would readily understand that a book with the term "data protection" in its title must address laws and policies designed to prevent abusive uses of personally identifiable information in the hands of businesses or the government.[12] However, no U.S. publisher could hope to sell a book emphasizing this term in its title because "data protection" does not resonate with the average American lawyer, much less with a general U.S. audience.[13]

Professors Paul M. Schwartz and Joel R. Reidenberg surely hoped that the title *Data Privacy Law*[14] would attract readers by emphasizing the book's concern with the privacy dimensions of collecting and using personal information. However, even this title is probably too cryptic for an American audience. Professor Peter P. Swire and Brookings scholar Robert E. Litan took a more journalistic approach to naming *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*.[15] With two references to privacy, two to the international scene, and one to electronic commerce, Swire and Litan seem to have hoped that prospective readers could, by triangulating these clues, guess the book's main theme. Public concern about threats to personal privacy arising from Internet transactions may be sufficiently strong[16] that an American reader could use his or her general (as opposed to legal) consciousness of this topic to grasp the issues with which *None of Your Business* is concerned.

For practicing lawyers whose clients engage in transborder data flows (and these days, whose do not?), the two books under review should become essential reading. They provide a rich and complementary framework for understanding data privacy laws and their practical implications. Both books also contribute to the public policy debate about data privacy, as well as to the emerging field of scholarship about it.[17]

Part I of this Book Review discusses Swire and Litan's *None of Your Business*.[18] Swire and Litan explain why Europeans and Americans have taken such different approaches to regulating private sector uses of

---

12 *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 5.

13. Schwartz and Reidenberg recognize that for American lawyers, the term "data protection" would likely conjure up the idea of intellectual property protection. *See id.* at 5-6.

14. SCHWARTZ & REIDENBERG, *supra* note 2.

15. SWIRE & LITAN, *supra* note 1.

16. *See id.* at 80 (citing polls regarding the American public's concern with data privacy).

17. For other noteworthy recent contributions to data privacy scholarship, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338 (1997); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996).

18. SWIRE & LITAN, *supra* note 1.

personal data.[19] They also discuss how European developments affect American industries.[20] Swire and Litan offer a detailed critique of the European data protection regime on the basis of its overbreadth, complexity, and inflexibility.[21] Although they hope that it does not become necessary to challenge the European data protection directive as a nontariff barrier to trade before the World Trade Organization, they foresee some circumstances in which such a challenge might be successful.[22]

Part II discusses Schwartz and Reidenberg's *Data Privacy Law*.[23] Schwartz and Reidenberg distill four basic elements from European data protection regulations.[24] The authors then systematically measure how well American law complies with these elements in the public and private sectors, both as a matter of state and federal law.[25] Throughout their book, Schwartz and Reidenberg display sympathy for these European norms. They accept European principles and rules as a given to which U.S. firms must adapt or face sanctions.[26] But they also believe that stronger data protection legislation would be good for the United States, even if they do not expect the United States to adopt precisely the same rules as the Europeans.[27]

In contrast to Swire and Litan, who offer a utilitarian rationale for the protection of personal data,[28] Schwartz and Reidenberg view data privacy as a civil liberty issue.[29] Each book's different conception of the nature of people's interest in data about themselves can be neatly illustrated by considering how each set of authors would deal with the idea of "propertizing" personal data as a way to protect such data in global digital networked environments. This is explored in Part III. Part III also argues that there are some situations in which it would be undesirable to commodify personal data.

---

19. *See id.* ch. 1.

20. *See id.*

21. *See id.* at 14-15.

22. *See id.* at 190-94. Joel Reidenberg is, however, skeptical that this will occur. *See* Electronic mail from Joel R. Reidenberg, Professor of Law, Fordham Law School, to Pam Samuelson, Professor of Law and of Information Management, University of California, Berkeley 2 (Jan. 4, 1999) (on file with author) [hereinafter Reidenberg E-mail].

23. SCHWARTZ & REIDENBERG, *supra* note 2.

24. *See id.* at 13-17.

25. *See id.* pts. II-III.

26. *See id.* at 392-400.

27. The authors' advocacy for stronger legal protection for personal data is occasionally evident in *Data Privacy Law*. *See id.* at 183. It is more clearly evident in other of their writings. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or a Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1991); Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997).

28. *See* SWIRE & LITAN, *supra* note 1, at 8.

29. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 30-32, 39-56.

Part IV offers some reflections on the data protection debate. The call for a new form of legal protection for personal data is one of a number of examples of information policy challenges that have arisen because of advances in information technologies. Understanding the parallels between data privacy and these other information policies may help policy makers and practitioners steer a sensible course through the uncharted waters of the information age. Part IV also suggests that European insistence on universalizing their approach to personal data protection could inadvertently undermine the European's goals.

I

None of Your Business: A UTILITARIAN APPROACH TO DATA PROTECTION

A central theme of *None of Your Business* emerges from the dual meaning of its title. By adopting a personal data directive with provisions affecting transborder data flows, Europeans are, in a sense, telling Americans that it is none of their business to collect information about European citizens (and implicitly that Americans ought to be more respectful of their own citizens' privacy rights).[30] However, many Americans think that it is none of the Europeans' business what American firms do with personal data on American soil.[31] An international debate on data protection issues has grown out of these divergent positions.

Interestingly, Swire and Litan sympathize with both positions. They agree with the Europeans that personal data should be protected from misuse,[32] and they regard Europeans as "hav[ing] a legitimate interest in making sure that other countries are not used as havens to deliberately circumvent the effect of European laws on European individuals."[33] Swire and Litan also think that American outrage about the extraterritorial reach of the Directive should be "tempered by recalling how Washington itself has acted in recent years to extend the reach of various laws beyond the country's border."[34] On the other hand, Swire and Litan agree with the American position that the European Directive is overbroad and may not work.[35] They also argue, consistently with the American position, that the Europeans should exempt from regulation certain routine data transfers that pose minimal risk of abuse, and that the Europeans should be receptive

30. *See* SWIRE & LITAN, *supra* note 1, at 3.
31. *See id.*
32. *See id.* at 8.
33. *Id.* at 19.
34. *Id.* at 3 n.6; *see also id.* ("Examples include application of antitrust laws, enactment of the Helms-Burton Law to impose sanctions against countries that do business with Cuba, and limits on the export of strong encryption products even to longtime allies.").
35. *See id.* at 70-74.

to self-regulation and the use of model contracts as a way to protect data in jurisdictions outside the European Union.[36]

This Part discusses Swire and Litan's explanations for the United States' and the European Union's very different regulatory approaches to data protection. It then considers the utilitarian rationale Swire and Litan provide for data protection. Much of their critique of the European regulations derives from the way these regulations deviate from utilitarian principles. Finally, this Part discusses three other reasons Swire and Litan give for questioning the European Directive. Those reasons concern the soundness of the Directive's conception of the information technology environment, its impact on innovation, and its enforceability in view of the global nature of information flows.

A. *The Different Approaches to Data Protection Taken by the United States and the European Union*

Among the intriguing questions discussed in *None of Your Business* is why the United States and the European Union take such different approaches to data protection.[37] According to Swire and Litan, one factor is the "different information cultures" of the two jurisdictions.[38] Americans generally favor a freer flow of information than do their European counterparts.[39] Perhaps even more different—and more significant for the data protection debate—are the regulatory cultures of the two jurisdictions.[40] Although Swire and Litan do not spell out the differences quite as starkly as this Book Review will do, one gets the impression from their book that despite the fact that both the United States and members of the European Union are advanced Western democracies, the regulatory cultures of these two jurisdictions could hardly be more different.

Here is the essence of these differences. First, Americans are generally more trusting of the private sector and the market. Rather than having the government adopt strict rules that industries may ignore or subvert, Americans would prefer it if firms would voluntarily adopt and abide by appropriate standards.[41] Second, Americans tend to believe in the power of the mass media to hold private sector abuses in check.[42] Third, Americans are inclined to think that technologies can contribute to the solutions of

36. *See id.* at 16-17.

37. *Data Privacy Law* also contains some discussion of the United States' and the European Union's very different approaches to data protection. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 206-12.

38. SWIRE & LITAN, *supra* note 1, at 153.

39. *See id.*; *see also infra* notes 143-148 and accompanying text.

40. *See* SWIRE & LITAN, *supra* note 1, at 153-54.

41. *See id.* at 12.

42. *See id.* at 10-11.

problems created by technologies.[43] Fourth, even when Americans are considering government intervention, they are much more inclined than Europeans to engage in a cost-benefit analysis of regulatory alternatives.[44] Identifying a market failure may suggest the need for government intervention, but Americans are more likely to ask whether possible unintended consequences of a proposed regulation would make the cure worse than the disease.[45] Fifth, Americans are more inclined to adopt reactive rather than proactive regulations. That is, Americans are generally disinclined to regulate until problems have actually occurred, and they prefer to tailor regulatory solutions to those problems rather than to adopt broad regulations anticipating problems yet to arise.[46] Finally, Americans are more prone to adopt regulations that give consumers information about private sector practices so that consumers can exercise their market power to shop for firms with good policies.[47] Once they have such information, Americans tend to think that the market will work things out. Consumers who are averse to reuses of their personal data will, according to this view, shift their business to firms that respect their privacy preferences.

The European regulatory culture differs considerably from the American model. First, Europeans tend to think of self-regulation as tantamount to no regulation, in part because individuals will have no remedy if firms violate self-imposed codes of conduct.[48] Second, Europeans prefer to err on the side of overprotection rather than on the side of underprotection.[49] The European data protection directive illustrates this preference. It strictly regulates the kinds of data that can lawfully be collected, the purposes for which the data can be collected, the uses that can be made of the data, and the length of time the data can be stored.[50] The Directive also mandates the development of institutional infrastructures to ensure that personal data receives the meaningful protection intended by the regulators in both the private and public sectors.[51] Third, Europeans tend to craft relatively narrow exceptions to broadly applicable rules. The European data protection directive, for example, contains relatively few and relatively

43. *See id.* at 9-10.
44. *See id.* at 7-8.
45. *See id.* at 8-9.
46. *See id.* at 9-18.
47. *See id.* at 12-13.
48. *See id.* at 159.
49. *See id.* at 153-54. It should be noted that the European Directive is not self-executing. National legislation must implement it and national authorities must interpret and enforce the rules set forth in the Directive. *See* Directive, *supra* note 1, art. 32. *See generally* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 487-88 (1995) (discussing the European principle of subsidiarity and national implementations of E.U.-wide directives in the data protection context).
50. *See* Directive, *supra* note 1, arts. 3-11.
51. *See id.* arts. 16-17, 28.

narrow carve-outs.[52] While the Directive's exclusion of certain governmental activities might seem to undercut this assertion, such exclusions derive partly from the European Union's lack of jurisdiction to regulate member state practices.[53]

Another deep-rooted difference between the United States' and the European Union's approaches to data protection arises from their different conceptions about the nature of people's interests in data about themselves. The European Directive includes data protection in its conception of the "fundamental rights" of citizens.[54] Although Americans cherish certain rights as fundamental to citizenship, they do not generally consider data privacy to be among them. Americans are more likely to cherish the principles embodied in the First Amendment—which favors a free flow of information—as fundamental human rights.[55]

B. Swire and Litan's Utilitarian Critique of the European Approach

In contrast to the European approach, Swire and Litan offer only utilitarian arguments for regulating private sector uses of personal data. They observe that at present, a firm has incentives both to acquire a wide range of information about individuals and to gain

> the full benefit of using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties. . . . Because customers often will not learn of the overdisclosure, they may not be able to discipline the company effectively. In economic terms, the company internalizes the gains from using the information but can externalize some of the losses and so has a systematic incentive to overuse it.[56]

This produces a market failure that is deepened by the seemingly intractable difficulties in successfully bargaining for the appropriate level of privacy. As Swire and Litan say:

> It can be daunting for an individual consumer to bargain with a distant Internet merchant or a telephone company about [uses of data about that individual]. To be successful, bargaining might take time, effort, and considerable expertise in privacy issues. Even then, the company might not change its practices. Even worse, a bargain once reached might be violated by the company, which knows that violations will be hard for the customer to detect.[57]

---

52. *See id.* arts. 8(2), 9.

53. *See id.* arts. 3(2), 13(1); SWIRE & LITAN, *supra* note 1, at 7.

54. *See* SWIRE & LITAN, *supra* note 1, at 3.

55. *Cf. id.* at 153 (discussing Americans' nearly religious attitude toward First Amendment rights).

56. *Id.* at 8.

57. *Id.*

Swire and Litan also consider whether data protection is needed to promote electronic commerce.[58] They suggest that one reason to adopt data protection regulations may be consumers' possible reluctance to do business on-line if they cannot control the uses that will be made of personal data collected during the transaction.[59]

Given their very utilitarian approach to data protection, it is not surprising that Swire and Litan are critical of the European Directive for its overbreadth. They consider, for example, the Directive's implications for laptop computers and personal organizers.[60] If an executive from the United States takes a laptop or a personal organizer with her on a business trip to Paris, she will, by the end of the trip, almost certainly have accumulated in it personally ideutifiable information about European citizens. Such information might include the executive's notes about what happened at the business meeting for which she made the trip or a list of persons to contact while in Paris.[61] The executive would be unpleasantly surprised if her laptop or personal organizer was seized at Charles DeGaulle Airport because of the personal data it contains, which United States law would inadequately protect. Yet, the Directive authorizes stopping this kind of flow,[62] even though the risk of abuse from the executive's possession of the data is relatively small.

Swire and Litan assert that the European Directive would also affect many other routine flows of data, such as those that occur within a transnational corporation (e.g., the distribution of a directory of employee telephone numbers or an organization chart identifying heads of the firm's departments) or those between a transnational company and its auditors or financial services agents.[63] Among the other organizations affected by the Directive are the press, educational institutions, international conferences, and Internet service providers.[64] All possess information identifiable to European individuals; they are therefore subject to the Directive.[65] Even e-mail from or about European colleagues is potentially subject to the

58. *See id.* at 76-79; *see also* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), *available at* <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (visited June 12, 1998) (identifying privacy as an important policy affecting electronic commerce).

59. *See* SWIRE & LITAN, *supra* note 1, at 77-78. However, Swire and Litan question how much of a hindrance to electronic commerce the absence of U.S. data protection laws really is. *See id.* at 80-85.

60. *See id.* at 70-74.

61. *See id.*

62. *See* Directive, *supra* note 1, art. 25(4).

63. *See* SWIRE & LITAN, *supra* note 1, at 90-102.

64. *See id.* at 122-24, 126-28, 136-38.

65. For example, unless registration forms for an international conference unambiguously ask for a registrant's permission to include her name on a list of conference attendees, the Directive would forbid its inclusion. *See id.* at 127-28.

strictures of the Directive.[66] Swire and Litan plead for the granting of exemptions for routine business activities that pose little risk of abuse.[67] They also call for an acceptance of self-regulatory measures as "adequate" to protect personal data in circumstances in which firms already have ample reasons to safeguard personally identifiable business information.[68]

While they could have devoted an entire book to elaborating on such examples and expressing predictable American outrage about European overreaching, Swire and Litan, for the most part, opt for a more pragmatic approach. They argue that "simple fairness, world trade laws, and economic self-interest all dictate that many data flows should proceed without interruption."[69] Recognizing the impossibility of resolving fundamental "information culture" differences between the United States and the European Union, they instead seek to find practical solutions that would satisfy the core concerns underlying the European Directive while not unduly encroaching on American prerogatives. They are especially hopeful that model contract clauses to protect personal data will satisfy E.U. adequacy standards for interfirm transfers.[70] As if attempting to dispel unrealistic European hopes, Swire and Litan repeatedly insist that the United States will not adopt a comprehensive data protection regime akin to that established in the E.U. Directive.[71]

C. *Other Reasons for Rejecting the European Approach*

Swire and Litan provide three additional reasons why the United States should not adopt a European-style mandatory data protection regime. First, the regulatory model embodied in the European Directive may already be outmoded in view of the emerging architecture of information technologies and networks.[72] Second, such a model may impede innovation.[73] Third, this sort of regime may be unenforceable given the global, decentralized digital networked environment to which it would apply.[74]

On the technology architecture issue, Swire and Litan observe that "[t]he Directive's approach is designed for the regulation of mainframe computers, in which one expects a relatively small number of hierarchical systems."[75] For example, the Directive relies heavily on each firm having a

66. *See id.* at 64-67.
67. *See id.* at 73-74.
68. *See id.* at 19, 66, 158, 168.
69. *Id.* at 19.
70. *See id.* at 164, 172-74. Schwartz and Reidenberg also discuss the use of contracts to satisfy the E.U. data protection "adequacy" standards. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 400-04.
71. *See* SWIRE & LITAN, *supra* note 1, at 16-17, 154, 173.
72. *See id.* at 50.
73. *See id.* at 78.
74. *See id.* at 144.
75. *Id.* at 50.

designated "controller" whose job includes overseeing and implementing data protection rules.[76] "Information technology, however, has shifted radically to new configurations such as client-server systems and the Interuet. Today there is a much larger number of systems organized into distributed networks rather than simple hierarchies."[77] In highly decentralized distributed systems, there is no central controller of information. Indeed, almost everyone connected to the network is a "controller" of personal data.[78] Although the Europeans realize that further work will be needed to articulate data protection in the context of the Internet,[79] there is reason to doubt that the mainframe-centric mandatory European model can successfully be applied to a distributed information environment.

Moreover, Swire and Litan point out that in an era of rapid technological change, complex mandatory rules could be harmful to innovation.[80] "[R]egulation would be drafted with existing practices in mind, without taking account of as-yet-undiscovered ways to do business. Promising experiments may have to be abandoned because they conflict with one or another of the rules."[81] Even if European officials were willing to make exceptions or adapt their mandatory rules to respond to new conditions, "the change could come too late to get the innovation to market, especially in markets in which product cycles are often measured in months."[82] Swire and Litan note that "[t]he dampening effect on innovation is especially acute for smaller and start-up companies. These companies typically are focused on their new products, and do not have much regulatory expertise in-house."[83] In this and other respects, Swire and Litan suggest that Europeans may find that the complex, mandatory data protection regime will put them at a disadvantage in a competitive world market.[84] Considerations of this sort help to explain U.S. reluctance to adopt the same regulatory model.

Swire and Litan also question whether the Europeans can exercise jurisdiction to enforce data protection—or other laws, for that matter—on the Internet.[85] Transnational cooperation among policy makers may be necessary to develop a workable set of regulations and practices in this and

76. *See* Directive, *supra* note 1, arts. 6(2), 10-12.
77. SWIRE & LITAN, *supra* note 1, at 50.
78. *See id.* at 66.
79. *See id.* at 66-67.
80. *See id.* at 78.
81. *Id.*
82. *Id.*
83. *Id.* at 78-79.
84. *See id.* at 151.
85. *See id.* at 144; *see also* Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998) (explaining why it will be easier to regulate the data privacy practices of large multinational organizations ("elephants") than those of smaller organizations ("mice") that may avoid penalties for misuse of data by shifting operations to new jurisdictions).

other areas. Swire and Litan view the European data protection directive as potentially providing "an early testing ground for the trans-national governance of the Internet and related information technologies."[86] They suggest that this transnational governance will only occur if the Europeans are willing to work toward an internationally satisfactory approach to data protection.[87]

II

Data Privacy Law: A CIVIL RIGHTS APPROACH TO DATA PROTECTION

Data Privacy Law is the culmination of a research project that Schwartz and Reidenberg undertook for the European Commission while the E.U. data protection directive was being considered.[88] The Commission had initially intended to use Schwartz and Reidenberg's report to inform its internal deliberative process, but eventually perceived in it an opportunity to apprise a U.S. audience about E.U. data protection principles.[89] The Commission's decision to support conversion of the report into a book aimed at a U.S. audience was a wise one. Now that the E.U. Directive applies in full force to data flows involving European citizens,[90] *Data Privacy Law* should be an invaluable resource to lawyers representing American firms that must conform their data protection practices to European requirements.

Because it was written before the E.U. Directive became final, *Data Privacy Law* does not discuss, let alone analyze at length, the text of the final Directive.[91] Some readers will undoubtedly wish that Schwartz and Reidenberg had revised their report to reflect this important development.[92] However, given that the European Directive only requires "adequacy" in data privacy practices, American lawyers will still benefit from Schwartz and Reidenberg's useful condensation of the core concepts of European data protection into four elements.

---

86. SWIRE & LITAN, *supra* note 3, at 4; *see also id.* at 182-83 (contrasting transgovernmental efforts to reach consensus on data protection with international governance via supranational, multilateral organizations, such as the United Nations). To enable the United States to participate effectively in such transnational governance efforts, Swire and Litan recommend the establishment of an Office of Electronic Commerce and Privacy Policy in the U.S. Department of Commerce. *See id.* at 16, 185.

87. *See id.* at 170-76.

88. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at xiii.

89. *See* Reidenberg E-mail, *supra* note 22.

90. *See* Directive, *supra* note 1, art. 32(1), 34.

91. A supplement to *Data Privacy Law* will contain a copy of the European Directive. *See* Memorandum from Paul Schwartz, Professor of Law, Brooklyn Law School, to Pam Samuelson, Professor of Law and of Information Management, University of California, Berkeley 3 (Jan. 4, 1999) (on file with author) [hereinafter Schwartz Memorandum].

92. Schwartz and Reidenberg intend to update *Data Privacy Law* to keep it current. A 1998 Supplement has already been published. *See id.*

This Part first describes the four elements of European data protection law that provide Schwartz and Reidenberg with a framework for analyzing how well U.S. law comports with European law in various sectors. Compliance with European law in the United States is sometimes inadvertent. This Part also discusses examples demonstrating deficiencies in U.S. compliance with the elements of European law, as well as the reasons for these deficiencies. Finally, this Part considers why Schwartz and Reidenberg think that U.S. law should recognize a right of information privacy that could protect personal data even when the possessor of the data collected it from independent sources.

A. *Four Elements of European Data Protection Law and How U.S. Law Compares*

Given how detailed and complex European data protection rules are, one must be grateful that Schwartz and Reidenberg found a way to distill the European approach into four basic elements. These elements are: (1) the creation of norms for collecting and processing personal information; (2) the establishment of an opportunity for affected individuals both to review information collected about themselves and to review the compiler's information practices; (3) the creation of special protection for sensitive data, such as data pertaining to ethnic origins, religion, or political affiliation; and (4) the establishment of enforcement mechanisms and oversight systems to ensure that data protection principles are respected.[93] Schwartz and Reidenberg exhaustively examine U.S. federal and state statutes, regulations, case law, and industry codes of ethics to determine the extent to which they are functionally similar to European-style data protection rules and practices.[94] In addition, they report on a survey they conducted about how various U.S. industries and industry associations handle personal data.[95] In both respects, *Data Privacy Law* complements the Swire and Litan book, which contains relatively little detail on the state of U.S. law or current industry practices.[96]

Data Privacy Law has three main parts: an elaboration of a conceptual framework for data protection regulations, an analysis of public sector data protection laws, and an analysis of private sector regulations and practices.[97] Within each chapter in the latter two parts, Schwartz and

93. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 13-17. These elements do not derive solely from the European Directive, but also from other European treaties and initiatives. *See id.* at 13.

94. *See id.* chs. 5-13; *see also id.* at 24-25 (discussing "functional similarity").

95. *See id.* at 26-28; *see also id.* app. A at 407-24 (reproducing the survey). Discussion of the survey's findings is woven into Part III of *Data Privacy Law*.

96. *See* SWIRE & LITAN, *supra* note 1, at 43 & n.31, 170-72 & nn.15-16 & 20 (mentioning *Data Privacy Law* and another study on the American data protection landscape).

97. Schwartz took primary responsibility for writing the chapters on U.S. constitutional law, federal statutes, state legislation, and regulations and practices pertaining to medical information. *See*

Reidenberg methodically assess U.S. compliance with each element of European fair information law. This style of presentation makes the book less than thrilling as a narrative, but very useful as a reference source. Without this book, many lawyers attempting to determine how the E.U. Directive might affect a particular client's data transfers would not even know where to begin their searches.

Schwartz and Reidenberg are particularly insightful in showing the fair information practice dimensions of some U.S. laws intended for purposes other than personal data protection. Their analysis of the U.S. Freedom of Information Act (FOIA)[98] provides an excellent example. The principal purpose of the FOIA is, of course, to promote democratic principles by providing Americans with a right of access to information in the hands of the federal government.[99] But the FOIA has other dimensions as well, including some that shield from unauthorized uses and disclosures personal information in the hands of U.S. agencies.[100] Two exemptions in the FOIA permit agencies to deny third party requests for personal data based on privacy considerations.[101] The FOIA also recognizes that especially sensitive data require special protection.[102] In addition, the FOIA provides persons with rights to access government-maintained data about themselves.[103] It also provides persons with rights to insist that these data be corrected, if they are in error.[104] Key aspects of the FOIA thus accord with three of the elements of European fair information law.[105]

In general, Schwartz and Reidenberg find more U.S. compliance with the first and third elements of European law (the data collection/reuse and sensitive data norms) than with the second and fourth elements (a right of review and enforcement norms).[106] They also find that the public sector complies with European fair information principles and practices more

---

SCHWARTZ & REIDENBERG, *supra* note 2, at 25-26. Reidenberg took primary responsibility for the chapters on fair information practices in the telecommunications, financial services, and direct marketing sectors of the U.S. economy, as well as in laws and practices that regulate private sector employment. *See id.* at 26.

98. 5 U.S.C. § 552 (1994), *discussed in* SCHWARTZ & REIDENBERG, *supra* note 2, at 108-14.

99. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 108.

100. *See id.* at 108-14.

101. *See* 5 U.S.C. § 552(b)(6)-(7), *discussed in* SCHWARTZ & REIDENBERG, *supra* note 2, at 109.

102. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 111-14.

103. *See id.* at 108. Schwartz and Reidenberg point out that this right of access is not limited to those to whom the data pertains. *See id.*

104. *See id.*

105. Defamation and equal employment opportunity laws are among the other U.S. laws that Schwartz and Reidenberg perceive to have fair information practice dimensions. *See id.* at 25.

106. *See id.* at 387.

than does the private sector,[107] with some notable exceptions in the regulation of private sector credit reporting and telecommunication services.[108]

Even so, the book provides some shocking stories of non-compliance with the first and third elements. For example, Johnson & Johnson has sold lists of five million elderly, incontinent women, and has defended such sales as consistent with industry practice.[109] Schwartz and Reidenberg point out that most firms actively engaged in compiling and marketing information about individuals do not inform the individuals that the data is being compiled about them, or about the uses the firms will make of the data.[110] "[I]f an individual requests to learn the source of personal information and the profile characteristics that were used for a marketing solicitation," Schwartz and Reidenberg report, "companies will [typically] either respond 'it's proprietary' or 'we won't tell you.'"[111] Consequently, Schwartz and Reidenberg favor greater transparency in private sector data collection and processing practices so that American public opinion can be mobilized to support policies that move in the direction of European-style data protection.[112]

Especially strong is *Data Privacy Law*'s discussion of the circumstances that have contributed to personal medical information being far more widely accessible and reused today than it was in the past.[113] Individuals were once able to rely on the professionalism of their doctors and the inefficiency of paper records as protections against the unauthorized use and disclosure of information about their health.[114] Until recently, computerized medical information tended to be in incompatible formats, making cross-correlation and reuse of this information difficult.[115] However, changes in the structure of the health care industry and further improvements in computerized medical information systems have fundamentally transformed the way in which personal medical information is gathered

107. *See id.* at 92-105.

108. Chapter 10 of *Data Privacy Law* discusses data protection in the telecommunications sector. *See id.* at 219-59. Section 11-2 of Chapter 11 discusses credit information sector regulations and practices. *See id.* at 286-306.

109. *See id.* at 171, 281, 336. Schwartz reports that Johnson & Johnson has finally ceased distributing this list. *See* Schwartz Memorandum, *supra* note 91, at 3. In a display of gender parity, Schwartz and Reidenberg point out that lists of impotent men have also been marketed widely. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 171.

110. *See id.* at 169-70, 329; *see also id.* at 388-90 (discussing the lack of transparency in the United States of most private sector practices as to the collection and processing of personal data).

111. *Id.* at 326; *see also id.* at 326-27 n.73 (describing some marketing firms' responses to Reidenberg's efforts to get such information).

112. *See id.* at 390.

113. *See id.* at ch. 7 (discussing medical information).

114. *See id.* at 158; *see also* Schwartz, *supra* note 27, at 12-18.

115. *See* Lynda Radosevich, *Health care uses XML for records: Other vertical industry groups also expected to cooperate to customize XML*, INFOWORLD ELECTRIC (Aug. 25, 1997) <http://www.infoworld.com/cgi-bin/displayStory.pl?/features/970825xml.htm> (discussing privacy implications of efforts to make medical information more interoperable).

and used. At least three clusters of persons now routinely process personal medical information: (1) those who engage in direct patient care (e.g., doctors, clinics, and nursing homes); (2) those who provide support for patient care (e.g., administrators, insurance services, and quality care reviewers); and (3) those who fall into the category of other secondary users of medical information (e.g., credential and evaluation personnel, public health officials, and direct marketers).[116] Both the burgeoning administrative oversight functions and the computerization of medical records have contributed to making medicine a true "'spectator sport.'"[117] In addition, Schwartz and Reidenberg point out that other novel health-related institutional structures—such as corporate-sponsored wellness programs—have privacy-threatening dimensions.[118]

Regardless of the sector within which they operate, American firms cannot safely ignore the European data protection directive. Schwartz and Reidenberg assert that every U.S. firm engaged in transborder data flows into and out of Europe will have the burden of proving that the rules in their jurisdiction and/or their own information practices satisfy E.U. standards.[119] This will be relatively easy in three instances: (1) if the firms operate in one of the few sectors already well-regulated by U.S. state or federal laws;[120] (2) if the data subject (i.e., the person about whom the data have been collected) has given unambiguous consent to collection and use of the data;[121] or (3) if processing of the data is a necessary incident to performance of a contract with the data subject.[122] The burden of proving the adequacy of a firm's data protection practices may also become lighter if the European Union agrees to accept U.S.-proposed "safe harbor" guidelines and model contract provisions as a way for non-E.U. firms to demonstrate the adequacy of their safeguarding practices.[123] However, no such agreement is yet in place. American firms thus have ample reason to worry about the impact of the European Directive on their transborder data flows.

---

116. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 159.

117. *Id.* (quoting Steffie Woolhandler & David U. Himmelstein, *The Deteriorating Administrative Efficiency of the U.S. Health Care System*, 324 NEW ENG. J. MED. 1253 (1991)).

118. *See id.* at 154. Corporate wellness programs may be useful to employers as ways to collect information about employee health; such information may then be used against the employees. *See id.*

119. *See id.* at 380-88, 396.

120. *See id.* chs. 10-11.

121. *See* Directive, *supra* note 1, art. 8(2)(a).

122. *See id.* art. 8(2)(b).

123. *See, e.g.*, Letter from U.S. Department of Commerce to Industry Representatives (Nov. 4, 1998) <http://www.epic.org/privacy/intl/doc-safeharbor-1198.html> (proposing "safe harbor rules"); *see also* Nadya E. Aswad, *Commentators Demand Clarity; Group Asks If Self-Certification Qualifies as Safe Harbor*, 3 Electronic Com. & L. Rep. (BNA) No. 45, at 1337 (Nov. 25, 1998) (discussing proposed safe harbor rules); Robert Gellman, *Commerce Department's Safe Harbor Proposal Sinks at the Dock*, DM NEWS, Dec. 21, 1998, at 15 (explaining why the Europeans are unlikely to accept these safe harbor rules).

B. *Schwartz and Reidenberg's Views on the Right to Information Privacy*

While this Book Review has thus far emphasized the deeply practical mission of *Data Privacy Law*, it would unfairly diminish Schwartz and Reidenberg's contributions to the American policy debate to dwell only on this aspect of their work. Schwartz and Reidenberg hope to do for data privacy at the end of the twentieth century something akin to what Brandeis and Warren did for the "right to be let alone" at the end of the nineteenth century.[124] Following in the footsteps of Brandeis and Warren, Schwartz and Reidenberg extract data protection principles from existing laws and legal decisions, many of which were adopted for very different purposes or justified on very different grounds.[125] Schwartz and Reidenberg believe that these principles can be used to build an American law of data privacy.[126] Like Brandeis and Warren, Schwartz and Reidenberg argue for establishing a new legal right of privacy by showing that existing law already contains the seeds of the right they advocate, and by arguing that extending the law in the manner they propose is just.[127]

It is fair to observe, however, that the data privacy rights for which Schwartz and Reidenberg argue are not privacy rights in the classic "right to be let alone" sense. Nor are they privacy rights akin to those recognized in U.S. Supreme Court rulings about intimate consultations between individuals and their doctors.[128] Some might argue that they really are not even privacy interests at all. If individuals voluntarily provide data about themselves to persons or firms outside the intimacy of the doctor-patient relationship, for example, some may regard the data as having been transferred out of the private realm. If instead firms have gathered data about individuals from other sources, especially from publicly accessible ones, the data will also seem non-private. In addition, firms that have paid for data about individuals will surely not regard the individuals as having any legally protectable interest in the purchased data. Indeed, as Schwartz and Reidenberg point out, firms that sell data about individuals to other firms tend to think that if anyone owns the data, the firms themselves do by

---

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

125. *See, e.g.*, SCHWARTZ & REIDENBERG, *supra* note 2, at 7-12 (discussing several sources of U.S. data protection law).

126. *See id.* at 12.

127. *See id.* at 36-43, 89-90.

128. *See* Whalen v. Roe, 429 U.S. 589, 599-600 (1977) (recognizing privacy interest in doctor-patient decision making abont prescription drugs, but holding that the statute at issue does not violate the constitutional right of privacy), *discussed in* SCHWARTZ & REIDENBERG, *supra* note 2, at 76-89; *see also* Kang, *supra* note 17, at 1202-03 (distinguishing between three kinds of privacy: spatial, decisional, and informational).

virtue of their investments in the development of such commercially valuable information assets.[129]

A society may, moreover, have reasons other than privacy concerns for imposing some legal responsibilities on firms that compile or market personal data. A society might, for example, confer on individuals a right to access and correct errors in credit reports in order to protect the integrity of the credit system, and not to protect privacy interests.[130] A society could also insist that credit report services maintain the confidential status of their reports in order to deter identity theft or other fraudulent conduct.[131]

So why do Schwartz and Reidenberg conceive of personal data in the hands of data compilers as a privacy issue? They do so, in part, because they see in the amalgam of U.S. privacy law a nascent American concept of *data* privacy.[132] They cite polls showing that an overwhelming majority of Americans think that their privacy is threatened by the large volumes of data about them that others possess.[133] These polls show that many people who disclose to others information about themselves for a particular purpose (e.g., to get credit or to be treated for a disease) believe that their disclosures have been made under an implied, if not an explicit, pledge to use the data only for that purpose.[134] This resembles the belief of trade secret owners that confidentially disclosing commercially valuable secrets to other firms creates an implied, even if not an express, pledge on the part of the other firms not to use the trade secrets except in a manner consistent with the limited purpose of the initial disclosure.[135] The law recognizes such expectations of trade secret owners. Why should it not also recognize individuals' privacy expectations regarding personal data?

The answer lies partly in privacy law's dependence on the reasonableness of the public's expectations.[136] Privacy tends to be protected best in cases in which courts decide that people have a reasonable expectation that their privacy *will* be respected in given circumstances.[137] Technological change may affect judgments about the reasonableness of these

129. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 326.

130. This is clearly part of the rationale for regulating credit reports. *See id.* at 286-301.

131. *See id.*; *see also* ELECTRONIC COMMERCE FIRST ANNUAL REPORT, *supra* note 11, at 17-18 (discussing concerns about identity theft and fraud).

132. *See supra* notes 125-127 and accompanying text. In this, they are not alone. *See* Kang, *supra* note 17, at 1202-08.

133. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 155, 312-13 (citing polls); *see also* SWIRE & LITAN, *supra* note 1, at 80 (same); Kang, *supra* note 17, at 1196-98 (same).

134. This seems to underlie people's sense that it is wrong for firms to make information about them into a salable commodity. *See* Kang, *supra* note 17, at 1197 n.12.

135. *See* SWIRE & LITAN, *supra* note 1, at 165 (noting similarities between data protection and trade secrecy law).

136. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 61-63.

137. *See, e.g.*, Minnesota v. Olson, 495 U.S. 91 (1990) (holding that a guest has a reasonable expectation of privacy while staying in a friend's home), *discussed in* SCHWARTZ & REIDENBERG, *supra* note 2, at 61 n.111, 62 n.113.

expectations. For example, advances in surveillance technologies have sometimes made previously private activities more transparent. This has affected court determinations about how reasonable it was for people engaging in those activities to expect the activities to remain private.[138] Schwartz and Reidenberg point out that the circular reasoning of U.S. decisions on privacy expectations "ignores the silent ability of technology to erode our expectations of privacy."[139]

Technology is, however, not the only—and perhaps not even the main—development that has contributed to a diminishment of the reasonableness of American expectations about personal data privacy. Industry has also played a large role. The last couple of decades has seen a very substantial expansion in the business of gathering, processing, and selling information about individuals in the United States.[140] Middle-class Americans are no longer surprised to receive an unsolicited copy of a catalog from Land's End or Pottery Barn. It is no secret that these firms must have received the names and addresses from some list they purchased from another firm. Given how widespread this practice is, it has perhaps become unreasonable for people to assume that the information they disclose to the businesses with which they deal will *not* be used for direct marketing purposes. Moreover, as direct marketing has become a more important U.S. information industry, it may have become more difficult (even if not more unreasonable) to expect legislators to adopt rules that would upset the expectations of these industries and alter industry practices.[141]

III

ESTABLISHING INDIVIDUAL PROPERTY RIGHTS IN PERSONAL DATA?

Direct marketers can also look to deep-seated tenets of American information policy to justify their trafficking in personal information. Although Schwartz and Reidenberg underplay the influence of First Amendment principles that favor the free flow of information as a way to

138. *See, e.g.*, United States v. White, 401 U.S. 745 (1971) (holding the use of electronic surveillance permissible because speaker had no reasonable expectation of privacy that listener would not be wearing an audio "bug"), *discussed in* SCHWARTZ & REIDENBERG, *supra* note 2, at 65.

139. SCHWARTZ & REIDENBERG, *supra* note 2, at 64.

140. *See id.* at 308. It is worth noting that this phenomenon has been substantially furthered by advances in technology that make it easier to collect and process this information. *See* Schwartz Memorandum, *supra* note 91, at 4.

141. This may help explain why the Clinton Administration has been so intent on promoting self-regulation as the best approach to data protection. *See* ELECTRONIC COMMERCE FIRST ANNUAL REPORT, *supra* note 11, at 16-17. Like so many other concepts, though, "privacy" is a social construct. Legislation can define as "private" information that society has concluded *should* be private, such as personal data about buying or reading habits.

promote a marketplace of ideas,[142] Swire and Litan point out that Americans have "an almost religious attitude toward free speech rights under the First Amendment."[143] This has spillover effects on the data privacy debate.[144]

The First Amendment is not the only American information law that values free flows of information. In 1991, the U.S. Supreme Court denied copyright protection to white pages listings in telephone directories.[145] It based this decision in part on the constitutional policy goal of copyright law, which favors free flows of information as a way to promote the progress of science and the useful arts.[146] Moreover, market-based economic theory posits that free flows of information promote perfectly competitive markets.[147] These components of the American "information culture" (to borrow a phrase from Swire and Litan[148]) tend to disfavor recognizing any legally protectable interests in an individual's data about herself. There is, however, some reason to think that this aspect of U.S. information culture may change.

One way it may change is if the United States follows the recommendation of a number of economists, Carl Shapiro and Hal Varian among them, who propose granting individuals property rights in their personal information as a way of resolving the data privacy controversy.[149] Shapiro and Varian perceive privacy as an externality problem: "I may be adversely affected by the way people use information about me and there may be no way that I can easily convey my preferences to these parties."[150] If individuals had property rights in information about themselves, they could convey their preferences to the market.[151] Those who valued their

142. The First Amendment is rarely mentioned or discussed in *Data Privacy Law. See, e.g.*, SCHWARTZ & REIDENBERG, *supra* note 2, at 6 (making an oblique reference to the First Amendment). When it is, the emphasis is on the extent to which the First Amendment may provide protection against compelled disclosure of one's affiliations with controversial organizations, such as the NAACP or the Ku Klux Klan. *See id.* at 44-49.

143. SWIRE & LITAN, *supra* note 1, at 153.

144. *See id.* at 153-54.

145. *See* Feist Pub. Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991).

146. *See id.* at 349-50; *see also* U.S. CONST. art. I, § 8, cl. 8 (suggesting that the primary purpose of copyright law is "[t]o promote the Progress of Science and useful Arts").

147. *See, e.g.*, James Boyle, *A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading*, 80 CALIF. L. REV. 1413 (1992) (discussing economic theories).

148. *See, e.g.*, SWIRE & LITAN, *supra* note 1, at 153-54.

149. *See* Carl Shapiro & Hal R. Varian, *US Government Information Policy* (July 30, 1997) <http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html>; *see also* Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92 (proposing property rights in personal data as a way to protect privacy).

150. Shapiro & Varian, *supra* note 149, at 16.

151. *See id.* There are two classes of people who might not exercise property rights in information: those who value privacy so highly that they will not want to engage in transactions for their personal information, and those who do not care about who has what information about them. But this does not undermine the idea of property rights in this kind of information, given that opting out of the private property system is always a choice one has in a market economy.

privacy highly could charge hefty prices for their data, while those who cared very little about data privacy could provide information about themselves to firms for little or nothing. The market, Shapiro and Varian suggest, can accommodate variations in individual preferences about information privacy just as it accommodates variations in preferences about tangible property.[152] The property rights approach has the advantage of addressing the information privacy problem without the need for government intervention.[153]

Given the fact that the market in personal information is already very substantial and personal data are commercially valuable,[154] the idea of granting individuals property rights in their personal information is perhaps not as radical as it might initially seem. Propertizing personal information would merely extend this market and give members of the public some control, which they currently lack, over the traffic in personal data. To service this new market, some commentators predict the rise of a new class of merchants—perhaps to be known as "infomediaries"—that will engage in transactions on behalf of individuals, many of whom have neither the time nor the inclination to negotiate directly with each firm wishing to make use of information about them.[155] Recognition of an individual property right in personal information might help fuel the emerging "attention economy" and electronic commerce along with it.[156]

Lawyers seem to have a more cautious reaction than economists to the property rights in personal information proposal. Swire and Litan do not endorse the idea of granting property rights in information as a means of protecting personal data, although they have no principled objection to it.[157] They perceive this approach as one possible means of achieving the desired end, although they regard it as one that requires further study before it is implemented.[158] Their main concern is to develop more immediate and pragmatic ways to respond to the European Directive, such as exempting certain low-risk transactions and promoting self-regulatory codes of conduct and model contract terms.[159]

---

152. *See id.* Varian points out elsewhere that many people value privacy because it protects them against annoying intrusions. *See* Hal Varian, *Economic Aspects of Personal Privacy* (Dec. 6, 1996) <http://www.sims.berkeley.edu/~hal/Papers/privacy.html>. However, many uses of personal information are not widely viewed in this way. There are surely some readers of this Book Review who do not mind, and may even welcome, unsolicited mail order catalogs.

153. *See* Shapiro & Varian, *supra* note 149, at 16. Legislators or courts would, of course, have to recognize property rights in personal information for the market to get started.

154. *See id.* at 16.

155. *See, e.g.*, John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, HARV. BUS. REV., Jan.-Feb. 1997, at 53.

156. *See, e.g.*, Michael H. Goldhaber, *Attention Shoppers!*, WIRED, Dec. 1997, at 182.

157. *See* SWIRE & LITAN, *supra* note 1, at 86-89.

158. *See id.* at 87.

159. *See id.* at 16-17, 73-74, 163-64, 172-73.

Schwartz and Reidenberg do not discuss the idea of granting property rights in personal information as a way to meet the "adequacy" standard of the European data protection directive, but one would gather from their book that they would disapprove of such an approach.[160] Like their European counterparts, Schwartz and Reidenberg emphasize that data protection is a civil rights issue.[161] They think that a free society depends on individual self-determination, autonomy, and dignity, which in turn depend on the right of the individual to control information about himself.[162] "The more that is known about an individual," they observe, "the easier it is to force his obedience."[163] This is why totalitarian societies tend to rely on information gathering as a way "to weaken the individual capacity for critical reflection and to repress any social movements outside their control."[164] Without even a hint of irony, Schwartz and Reidenberg proffer Germany as an example of a society that gives constitutional status to personal data protection as a precondition for self-determination and appropriate civic participation.[165] Schwartz and Reidenberg discern similar principles in some U.S. constitutional cases protecting associational privacy[166] and voting rights.[167] For those who embrace the civil rights concept of data privacy, the notion of protecting personal data by commodifying it would likely be as obnoxious as the notion of protecting the voting franchise by commodifying it.[168] Even if such a measure would promote high voter turnout, propertizing the voting franchise would be fundamentally destructive of the civil liberty interests the franchise is meant to protect.[169]

There are also strong policy reasons for recognizing some spaces within which information should not be commodified.[170] For example, if

160. In commenting on an earlier draft of this Book Review, both Schwartz and Reidenberg indicated that they do not, in fact, disapprove of propertizing personal information as a way of satisfying the adequacy standard of the E.U. Directive. *See* Reidenberg E-mail, *supra* note 22, at 2; Schwartz Memorandum, *supra* note 91, at 2. However, nothing in their book suggests this. Schwartz has elsewhere explored the possibility of establishing a "privacy market" in personal health information. *See* Schwartz, *supra* note 27, at 41.

161. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 39-42.

162. *See id.*

163. *Id.* at 39.

164. *Id.*

165. *See id.* at 41-43.

166. *See id.* at 43-53 (discussing such cases as *Roberts v. U.S. Jaycees*, 468 U.S. 609 (1984), and *NAACP v. Alabama*, 357 U.S. 449 (1958)).

167. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 53-59 (discussing such cases as *Storer v. Brown*, 415 U.S. 724 (1974), and *Reynolds v. Sims*, 377 U.S. 533 (1964)).

168. *See generally* MARGARET JANE RADIN, CONTESTED COMMODITIES (1996) (discussing rationales for not commodifying some values).

169. *See generally* SCHWARTZ & REIDENBERG, *supra* note 2, at 53-59 (discussing voting rights law). *See also* Pamela S. Karlan, *Not by Money but by Virtue Won? Vote Trafficking and the Voting Rights System*, 80 VA. L. REV. 1455, 1457 (1994) (arguing that the "real dangers of vote trafficking . . . [lie] in their distortion of postelectoral representation and governance").

170. *See, e.g.*, Pamela Samuelson, *Information as Property: Do* Ruckelshaus *and* Carpenter *Signal a Changing Direction in Intellectual Property Law?* 38 CATH. U. L. REV. 365 (1988)

Donald Trump and Elizabeth Taylor had unlimited property rights in information about themselves, they might rely on those property rights to stop the publication of unauthorized biographies, or even critical news stories about them. First Amendment civil liberty and copyright policy values that favor certain kinds of free flows of information should be maintained in these sorts of cases.[171]

IV

REFLECTIONS ON THE DATA PROTECTION DEBATE

Information technologies have posed a number of significant challenges to existing legal regimes in recent years. One such challenge has been to decide whether society can adapt existing legal norms to encompass new phenomena or whether new legal norms are needed instead.[172] A second challenge has been to temper the inclination to regulate in cases in which new technologies present seemingly unprecedented threats.[173] Policy makers have generally been more aware of the dangers of underregulation than those of overregulation.[174] Consequently, they have sometimes chosen to adopt strict and broadly protective rules that unintentionally threaten to stifle desirable developments.[175] A third challenge has been to formulate regulatory strategies that can be adapted in a rapidly changing technological and business environment.[176] A fourth has been to preserve cherished

---

(criticizing Supreme Court decisions containing overbroad pronouncements about property rights in information). Personal data is certainly one example of information becoming a commodity in the information age, but others might be given as well. *See, e.g.*, Joel Rothstein Wolfson, *Contract and Copyright Are Not at War: A Reply to "The Metamorphosis of Contract into Expand,"* 87 CALIF. L. REV. 79 (1999) (discussing markets in stock prices and similar data).

171. Even within a proprietary rights regime, doctrines sometimes permit unauthorized reuses of information for socially beneficial purposes, such as the fair use doctrine that privileges some reuse of copyrighted works for purposes of news reporting, criticism, and democratic discourse. *See* 17 U.S.C. § 117 (1994). *See generally* Jay Dratler, Jr., *Distilling the Witches' Brew of Fair Use in Copyright Law*, 43 U. MIAMI L. REV. 233 (1988) (discussing copyright's fair use doctrine and caselaw). A similar limiting doctrine might be needed if personal data becomes "propertized."

172. A good non-privacy example is whether computer programs should be protected by existing intellectual property regimes or whether they would best be protected by a "sui generis" regime. *See, e.g.*, Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308 (1994) (discussing a sui generis regime for protecting computer software).

173. A non-privacy example of this tendency is the "digital agenda" that the United States and the European Union pursued at an international level to respond to the challenges posed by digital technologies for copyright law. *See, e.g.*, Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369 (1997) (discussing this digital agenda).

174. *See generally* Shapiro & Varian, *supra* note 149, at 17-18 (discussing indecency and encryption regulations).

175. *See, e.g.*, Reno v. ACLU, 521 U.S. 844 (1997) (striking down overbroad regulation of indecent communications on the Internet).

176. One of the few policy documents seeming to recognize this challenge is the United States' A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE. CLINTON & GORE, *supra* note 58; *see also* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (discussing the challenges of regulating information technology developments).

human values in the face of strong economic pressures and technologies capable of undermining those values.[177] A fifth has been to find an internationally acceptable approach to regulation so that commerce and communication can proceed on a global scale without undue impediments that result from uneven regulatory environments.[178] Especially of concern is the potential emergence of "renegade" nations in which all sorts of illicit materials—unauthorized compilations of personal data, illicit copyright materials, pornography, and the like—would be readily available.

Each of these challenges has been evident in the international data protection policy debate discussed in this Book Review. Although data protection regulations are not a wholly new phenomenon, two recent developments have given them a new urgency. First, technological advances have made it much easier and much less expensive to amass and process large quantities of data. Second, personal data have acquired a new commercial significance, as both books under review attest.[179] Swire and Litan argue that Europeans have overreacted to the dangers of underprotection of personal data by adopting an overbroad and complex mandatory scheme that will have undesirable consequences, such as impeding innovation and economic growth in the European Union.[180] They also question whether the European approach to data protection is workable given the profound shift in the technological environment to decentralized networked distributed systems.[181] Yet, Schwartz and Reidenberg point out that Europeans have made an important contribution in identifying human values of data privacy that should be preserved in the new technological environment, even if this requires regulatory intervention that might have non-trivial economic consequences.[182] The European approach to gaining international compliance with its data protection regimes may have been somewhat high-handed (e.g., threatening to stop flows of data into countries lacking "adequate" protection for personal data). But one must admit that the Europeans have gotten the attention of U.S. and other national policy makers, and have established their approach as the benchmark against which other proposals are being measured.[183]

---

177. *See, e.g.*, A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995) (discussing the values at stake in the encryption policy debate).

178. *See, e.g.*, A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE (Brian Kahin & Charles Nessen eds., 1997).

179. Both books under review begin with observations about the impact of information technologies on the new urgency for data privacy regulations. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 1; SWIRE & LITAN, *supra* note 1, at 1-2; *see also* Kang, *supra* note 17, at 1220-40 (detailing automated data collection in digital networked environments).

180. *See supra* notes 80-84 and accompanying text.

181. *See supra* notes 75-78 and accompanying text.

182. *See* SCHWARTZ & REIDENBERG, *supra* note 2, at 1-2.

183. *See* SWIRE & LITAN, *supra* note 1, at 1-4.

This Part discusses some of the ways in which the challenges posed by data privacy parallel the challenges that have recently arisen in other information policy domains. It then argues that European insistence on universalizing their approach could lead to the undermining of the European's goals.

A. *Parallel Challenges in Other Information Policy Domains*

Although data protection is important, those concerned with this policy debate should realize that parallel challenges have arisen in other information policy domains in recent years.[184] Intellectual property law has been in the vanguard of legal regimes challenged by advances in information technologics. At least two new forms of intellectual property law have recently been enacted to respond to the challenges of information technologies: one to protect the layout designs of semiconductor chips,[185] and the other to protect the contents of databases.[186] A third possible new form of intellectual property protection is the proposal to "propertize" personal data as a way to protect privacy interests of individuals.[187] Existing intellectual property laws have also been stretched in other ways to respond to information technology challenges.[188]

Advances in information technology, as well as a seeming "gap" in intellectual property law that provides little or no protection to certain kinds of commercially valuable information, have also given rise to a recently proposed commercial law to regulate transactions in computer information. This proposed law is known as Article 2B of the Uniform Commercial Code.[189] Oddly enough, Article 2B and data protection

---

184. For example, one might add cryptography and communications policy to the list of information policies that recently have been challenged by information technologies, as the Clipper Chip initiative, *see* Froomkin, *supra* note 177 (explaining the Clipper Chip initiative), and the Communications Decency Act, 47 U.S.C. § 223 (West Supp. 1998), bear witness. *Reno v. ACLU*, 521 U.S. 844 (1997), held that the portions of the Communications Decency Act—including those that prohibit indecent communications on the Internet—are facially overbroad.

185. *See* 17 U.S.C. § 901-914 (1994).

186. *See* Council Directive 96/9, 1996 O.J. (L77) 20 (setting forth rules on the legal protection of databases). Some assert that databases need a new form of legal protection because digital information can be appropriatcd so much more easily, rapidly, and cheaply than in the print environment, which tends to undermine incentives to invest in database development. *See id.* Recitals. For critical commentary on the overbreadth of the database directive, see J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997).

187. *See supra* notes 149-156 and accompanying text.

188. *See, e.g.*, Samuelson et al., *supra* note 172, at 2343-64 (showing that copyright and patent law concepts have been stretched to adapt to the legal protection of computer software).

189. U.C.C. art. 2B (Draft, Dec. 1, 1998). As of this writing, the most recent draft of Article 2B is dated December 1, 1998. All versions of Article 2B are available on the Internet. *See* National Conference of Commissioners on Uniform State Laws, *Drafts of Uniform and Model Acts Official Site* (visited Jan. 28, 1999) <http://www.law.upenn.edu/library/ulc/ulc.htm>. Concerning the origins of Article 2B, see Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827 (1998) (arguing that information technology

policies may intersect if a transfer of personal information to a private sector firm via computer falls within the definition of a transaction in computer information under Article 2B.[190] This would make it subject to all of Article 2B's default rules, such as those concerning contract formation, scope of license, warranties, and remedies.[191] The drafters of Article 2B may never have contemplated this use of their regulatory regime, but in the free-for-all of the new information policy environment, should the reach of this model law necessarily be constrained by what its drafters might have intended?

The question is far from frivolous. Among the unseen dangers arising from the current haste to regulate the Internet and other new information technologies is that laws adopted to achieve one set of policy objectives may lose their coherence and capacity to guide human conduct if stretched to deal with new technology problems.[192] Economists may perceive a benefit in propertizing personal information in order to promote a market in which individuals can convey their privacy preferences to those who want the individuals' information. But the coherence of intellectual property law may be undermined if it is extended to establish a new property right in information that does not aim "to promote progress in Science and [the] useful Arts."[193] Similar unforeseen distortions may occur if Article 2B is unthinkingly extended to cover transfers of personal information.

An additional problem is that new laws taking a comprehensive approach to data protection may lack enough grounding in experience to enable their successful implementation.[194] One serious impediment to the

---

developments gave rise to the need for a new model commercial law to regulate transactions). *See generally* Symposium, *Intellectual Property and Contract Law for the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 87 CALIF. L. REV. 1 (1999) (exploring potential conflicts between intellectual property law and Article 2B and how such conflicts might be resolved); Symposium, *Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 13 BERKELEY TECH. L.J. 809 (1998) (same).

190. *See* U.C.C. § 2B-103 (Draft, Dec. 1, 1998) (indicating that Article 2B applies to computer information transactions).

191. *See, e.g.*, *id.* art. 2B pts. 1-2, 4, 7.

192. *See, e.g.*, Pamela Samuelson, *Intellectual Property and Contract Law for the Information Age: Foreword to a Symposium*, 87 CALIF. L. REV. 1, 3-4 (1999) (discussing this problem as it relates to Article 2B); *see also* A. Michael Froomkin, *Article 2B as Legal Software for Electronic Contracting—Operating System or Trojan Horse?*, 13 BERKELEY TECH. L.J. 1023, 1026 (1998) ("One reason why Article 2B has proven to be so difficult to get right is that the information technologies to which it would apply are themselves in a state of ferment.").

193. U.S. CONST. art. I, § 8, cl. 8; *see also* Rochelle C. Dreyfuss, Warren & Brandeis Redux: Finding (More) Privacy Protection (unpublished manuscript, on file with author) (expressing doubts about the usefulness of intellectual property law and principles to protect privacy); Kang, *supra* note 17, 1246-58 (explaining why a property rights approach may not be an optimal way to protect information privacy).

194. *See, e.g.*, Froomkin, *supra* note 192 (questioning whether Article 2B has sufficient grounding in experience to regulate the information economy).

adoption of European-style data protection rules in the United States derives from the lack of American experience with such laws and practices.

B. Reflections on Possible Disputes Between the United States and the European Union

While American information culture may in time embrace a conception of personal data as a civil liberty issue, it must be said that this view does not have broad support within the United States at present. Swire and Litan are correct in asserting that the U.S. Congress will not be persuaded to adopt a comprehensive mandatory scheme akin to the European Directive.[195] Even if adopted, such legislation would be unworkable because it would so clearly run counter to the American information culture and standard business practices. Far better is the idea of seeking pragmatic solutions to data protection problems, such as those explored by Swire and Litan in *None of Your Business*.[196] Such solutions would move American industry practices and its information culture toward greater protection of personal data. If over time Americans come to perceive personal data protection as a civil liberties issue, the law can adapt to this as well. Schwartz and Reidenberg suggest that this evolution is farther along than many Americans might have guessed.[197]

It would be a sad and ironic development if the dispute between the United States and European Union over data protection regulations ended up before the World Trade Organization (WTO). As Swire and Litan observe,

> there are reasons to be cautious about giving the WTO a leading role in resolving privacy disputes. In the resolution of [this sort of] dispute, it is far from clear that the organization is the most appropriate and expert decisionmaking body. It must decide how the challenged rule fits within WTO rules, rather than whether the privacy law is actually desirable.[198]

The Europeans have rightly realized that an information society should be about more than just trade. Let us hope that they care enough about gaining recognition for stronger protection of personal data in the international community that they will not inadvertently undermine their goal. The Europeans might inadvertently do this if they are so insistent on universalizing their approach to data protection that the United States decides it has no choice but to put the data protection dispute before the one

195. *See supra* note 71 and accompanying text.

196. *See supra* notes 69-70 and accompanying text.

197. Many Americans would likely be surprised, as this author was, that there was enough U.S. privacy law that Schwartz and Reidenberg could devote more than 400 pages to discussing it.

198. SWIRE & LITAN, *supra* note 1, at 194.

international tribunal whose sole raison d'être is the promotion of free trade.