Harvard Journal of Law & Technology
Volume 12, Number 3 Summer 1999

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.
<http://www.brookings.edu/press/inprint.htm>
Pp. 268. $39.95 (hard). ISBN 0-8157-8240-3.

I. INTRODUCTION

The European Union (EU) privacy Directive[1] went into effect on October 25, 1998, with little fanfare and without disrupting the voluminous flows of electronic data that daily cross the Atlantic ocean. As part of the effort to harmonize commerce and privacy rights within Europe, the Directive is not a radical departure from existing privacy laws in countries such as France, Germany, and Sweden. The Directive has attracted attention in North America because of its prohibition on the transfer of electronic data to non-EU ("third") countries that fail to ensure an "adequate level of protection".[2] Such a prohibition would be Europe-wide, not merely from a single EU country. As a result, businesses on both sides of the Atlantic fear that while October 25th may have come and gone without the sky falling, the potential disruptive effects of the Directive are looming on the horizon.

Not since the seminal 1890 article by Warren and Brandeis[3] has a single document so richly focused the debate on privacy rights and legitimate privacy expectations. When compared with American jurisprudence, the European Directive highlights significant differences in privacy against the government, privacy against society, and fundamental notions of "consent." This debate comes at a time in which the information explosion has reached unparalleled levels, both through conventional media and the Internet. New technologies further

---

1. European Union Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. (L 281) 31. A complete copy of the Directive is included as Appendix A of the book (pp. 213–46).

2. *Id.* at art. 25.

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

complicate the discussion by giving the average person unimaginable reach in obtaining information and at the same time creating significant unprotected exposure and with it the potential for privacy violations ranging from minor to horrific. In *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Peter Swire and Robert Litan join the debate with an insightful discussion and analysis of the Directive and its potential impacts. *None of Your Business* sets the stage for a classic confrontation between the world's two economic superpowers, Europe and the United States, by demonstrating they are on a collision course over privacy. The authors offer both broad and specific policy recommendations for public and private actors on both sides of the Atlantic to avoid disaster. They articulate several useful compromises between the reach of privacy protection possible under the Directive and the scope of privacy protected in America.

II. LEGAL CONTEXT OF THE DIRECTIVE

Following a brief introduction and overview of the text, *None of Your Business* opens with a discussion of the legal context of the Directive. The German and French national approaches to privacy are discussed (pp. 22–23) and the authors' delineate that "[t]he Data Protection Directive is designed to further the creation of a unified market in Europe" (p. 25). However, while the "Directive increases the free flow of information within the European Union," (p. 25) there is significant concern about the "effects of the Directive on flows of personal information from Europe to the rest of the world" (p. 24). In this sense, the "EU Directive represents a dramatic increase in the reach and importance of data protection laws" (p. 24). Thus, in a classic understatement, the authors' assess that "[t]he Directive is sweeping" (p. 26). Much of the rationale for the Directive's extraterritorial sweep is to prevent the circumvention of privacy laws by the creation of "data havens" outside of Europe that allow the very practices the Europeans have prohibited (p. 26). The authors' discuss the data protection requirements of the Directive (pp. 28–31) and specific requirements such as mandatory disclosure to the "data subject" and limitations on the "secondary use" of data. They then explore how the Directive could be implemented to prohibit transfers of data to "third" countries (non-EU states) for failing to provide "adequate" protection (pp. 31–34). It is here that we begin to see how the conflict over privacy may be averted. First, the authors suggest that there is a great deal of flexibility in interpreting adequacy, and that because the assessments are

to be made "in the light of all the circumstances,"[4] less protection may be required for less sensitive data (p. 32). Similarly, they suggest that the EU is unlikely to issue an across-the-board finding that U.S. privacy protections are inadequate. Instead they are likely to make adequacy determinations on a sector and practice-specific basis. The authors offer the example of the Fair Credit Reporting Act[5] as likely providing adequate protection to "allow transfers of credit information for credit, insurance, or employment purposes, even if transfers for other sectors were prohibited" (p. 32). Lastly, the language of the Directive does not require legal assurances to make a finding of adequacy; "professional rules and security measures which are complied with"[6] would also be adequate. This sets the stage for the use of contractual agreements and self-regulatory measures (SRMs) by businesses to comply with the mandates of the Directive.

Swire and Litan introduce the exceptions to the Directive, under which data transfers would be allowed regardless of a finding of adequacy. These include unambiguous consent, necessary for the performance of a contract, a contract in the interest of the data subject, legal claims and public interest grounds, vital interests of the data subject, transfers from public records, and adequate safeguards or SRMs (pp. 34–38). Much of the book is dedicated to encouraging businesses and European officials to adopt broad use of SRMs. While there is some discussion about the nature of both privacy and consent under the Directive, the authors do not spend significant time detailing the differences between the European and American expectations. They do indicate that "discussions with European officials suggest an understanding of the [consent] provision that would not be apparent to most American readers" (p. 34), but they do not contrast the European view with what is found in American jurisprudence. For example, under the Directive, "consent must be given 'unambiguously,' an apparently strict standard . . . . [and] consent to the proposed transfer requires consent to the *particular uses* to which the data will be put" (p. 34). In Chapter 6, "Financial Services Sector," the authors lay out some of the challenges to obtaining unambiguous consent, particularly if the Europeans require consent for each and every reference to a data subject, rather than allowing broad consent.

While the authors make the case for broad consent by demonstrating undesirable hassle both to businesses (particularly with

---

4. European Union Directive 95/46/EC, *supra* note 1, at art. 25(2).
5. 15 U.S.C. § 1681 (1994).
6. European Union Directive 95/46/EC, *supra* note 1, at art. 25(2).

regard to their employees) and individuals, a jurisprudential comparison with the United States Supreme Court's view of consent would also be insightful. For example, in *Smith v. Maryland*[7] the court announced that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"[8] and thus concluded that "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[9] The Court's ruling can be construed as holding that the defendant knowingly consented to have the phone numbers he dialed recorded and therefore consented to allow these to be passed on to a third party. Such a broad interpretation of consent is clearly not within the contemplation of the privacy Directive. In contrast, Justice Stewart's dissent in *Smith v. Maryland* expresses some of the very concerns that the Directive is intended to address. "I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[10] Thus we see sharp contrast with and sympathy towards the goals of the Directive in American jurisprudence.

Similarly, in a more recent decision, *U.S. Department of Justice v. Reporters' Committee*,[11] the Court explores the evils that can arise from abuse of computerized data banks, and the clash between the Freedom of Information Act[12] and The Privacy Act of 1974.[13] The Court observed that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[14] This difference is reflected in the Directive's limited application to "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic

---

7. 442 U.S. 735 (1979).
8. *Id.* at 743–744.
9. *Id.* at 744.
10. *Id.* at 748 (Stewart, J., dissenting).
11. 489 U.S. 749 (1989).
12. 5 U.S.C. §552(b) (1994).
13. 5 U.S.C. §552(a) (1994).
14. *Reporters' Comm.*, 489 U.S. at 764.

means of personal data which form part of a filing system" (p. 67).[15] There is a general recognition on both sides of the Atlantic that centralized information is more dangerous than limited, dispersed information. Where this consensus breaks down is in restricting the use and release of such information by private actors as opposed to the government. Thus the concern about abuses of centralized databases in the U.S. is focused on the government. The American obsession with freedom of information can be characterized as a holdover from "[t]he generation that made the nation [that] thought secrecy in government one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to."[16] Much of the American project with regard to privacy has been as privacy against the government. For example, the Bill of Rights provides an enumeration of freedoms from the government, not rights against other private actors. In contrast, the Orwellian fears of the Europeans seem less focused on government and more on private corporations.

This is not to say that the American experience has not afforded any protection to an individual's privacy against non-governmental actors. In *Olmstead v. United States*, Justice Brandeis vigorously dissented in a 5-4 decision to allow wire-tapping, because "the right to be let alone . . . [is] the most comprehensive of rights and the right most valued by civilized men."[17] Brandeis's view eventually won the day in *Katz v. United States*.[18] More recently, the Court has acknowledged that "there *is* a zone of privacy surrounding the individual, a zone within which the State may protect him from intrusion".[19] Further, as the *Reporters' Committee* Court noted, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[20] Yet, whether such control would be considered "adequate" under the Directive is not discussed in *None of Your Business*. The authors only suggest that the Directive will be like a 400 pound gorilla in setting privacy standards, whether they be done through government intervention or self-regulation. A discussion of the American

---

15. European Union Directive 95/46/EC, *supra* note 1, at art. 3(1).
16. *Reporters' Comm.*, 489 U.S. at 772–73.
17. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
18. 389 U.S. 347 (1967).
19. Cox Broadcasting Corp. v. Cohen, 420 U.S. 469, 487 (1975).
20. *Reporters' Comm.*, 489 U.S. at 763.

predisposition on these matters would have further enriched *None of Your Business*.

The authors spend some time discussing "why what is legal under the Directive matters" (pp. 45–49). "Many businesspersons have expressed the view that 'they just can't do that' — the European Union will simply not be willing or able to enforce the Directive as written" (p. 156). In contrast, the authors contend that the Directive's broad sweep has the potential to disrupt standard practices for accounting, investment banking, and even the press. Thus while the Directive may only be enforced in a discretionary manner, this provides little comfort to businesses operating in Europe that are technically out of compliance. "It may be risky for a company to create [a data processing] system in a way that seems forbidden by the language of the law but is allowed under the discretion of the *current* officials" (p. 47) (emphasis added). The authors argue that the Directive needs to be clearly interpreted to provide businesses and other data-exporters with notice so that they can avoid the public criticism and embarrassment that comes with noncompliance. "It is no trivial decision to adopt a deliberate corporate policy of noncompliance" (p. 47).

III. DATA PROTECTION, TECHNOLOGY, AND ENFORCEMENT

Following an admonition for European officials to be transparent in interpreting and applying the Directive, *None of Your Business* explores various technology and business sectors and how they could potentially be affected by the new regime. Noting that the "practical application of the Directive varies widely for different sorts of information technology," (p. 51) Swire and Litan examine ramifications for mainframes, client-server systems, company intranets, the Internet, email, facsimiles, the World Wide Web, and laptop computers, (pp. 50–75) and engage in a discourse on the effects of data protection laws on electronic commerce in general (pp. 76–89). They discuss potential effects of the Directive on various business sectors, including: human resources (pp. 90–94), auditing and accounting, (p. 94–97), consulting (pp. 97–98), customer service centers or call centers (pp. 98–99), and the financial services sector in general (pp. 102–21). They then explore possible impacts on the press (pp. 122–24), non-profits, educational institutions, and international organizations (pp. 125–28), the travel industry (pp. 132–36), Internet service providers (pp. 136–38), and direct marketers (pp. 138–44). In Appendix B, the authors supplement this analysis with a true gem. They provide an excellent and concise guide, organized by business and technology sectors, to the potential

effects of the Directive and potential exceptions, citing specific Directive articles applicable and means of compliance (pp. 247–60). In the course of these discussions the authors brilliantly anticipate the readers' questions. For example, they consider whether the Directive would apply to the exportation of information regarding a credit card purchase by an American in Europe (and conclude that it could) (pp. 105–06).

One of the insights of the book is that the Directive will apply to data regarding employees, not just customers (p. 60). The authors also suggest how the Directive could apply against non-business entities such as NATO, the United Nations, churches, news organizations, or even foreign governments conducting activities in Europe (pp. 42–43, 125–29). In addition, they examine the impact on businesses that make use of customer preferences, such as world-wide reservation services (pp. 133–35). Limitations on businesses' ability to tailor their services to match customer profiles could be debilitating as "[k]nowledge is an increasing portion of the value of an offering in the market place and the basis for competitive advantage."[21] Similarly, in the discussions about consumer confidence in use of the Internet and electronic commerce in general, they are quick to distinguish between *security* concerns and *privacy* concerns (pp. 81–83). Much concern about use of the Internet has largely been focused on security (e.g. protecting one's credit card numbers). However, as technological fixes, such as better encryption programs (p. 82), have alleviated this problem, users are beginning to refocus concern on protecting privacy.[22] Thus, proponents of the Directive argue that it will actually spur on electronic commerce. The authors concede that perhaps the data protection rules should be tailored to those areas in which individuals fear that sensitive data will be revealed in order to have the greatest effect on promoting electronic commerce, without inhibiting growth in other areas (p. 87). However, they conclude that although privacy may be a worthwhile end in and of itself, it is not likely to promote electronic commerce. In other words, the gains are outweighed by the harms (p. 89).

Of particular concern to the authors is that the introduction of a strict privacy regime through the Directive may inhibit the development of electronic commerce over the Internet. They warn that trying to tailor a statutory regime to a technology that is still in its infancy may

---

21. STAN DAVIS & JIM BOTKIN, THE MONSTER UNDER THE BED: HOW BUSINESS IS MASTERING THE OPPORTUNITY OF KNOWLEDGE FOR PROFIT 22 (1994).

22. *See, e.g.*, Ross Kerber, *Raytheon Suit Spurs Call for On-line Privacy Rules*, BOSTON GLOBE, Apr. 5, 1999, at A1.

either suffocate it or prove irrelevant as the technology takes unexpected turns (p. 78). "The up-to-date thinking underlying the statutes can quickly seem out of date" (p. 206). As the authors' hint, the entire privacy regime proposed by the Directive can be heralded as an example of law being unable to keep pace with and anticipate technological change. It was clearly drafted in and for an era in which our planet was less interconnected and interdependent. It is better equipped to address the large-scale data collection and processing that occurs in a few mainframe computers (pp. 52–58). These mainframes are easy to identify and enforce rules against. As a result, SRMs may prove particularly effective to addressing the use of mainframe computers. However, in light of modern technology, the Directive begins to look like a blunderbuss shot, covering applications such as "routine data processing that [were] likely not intended to be covered by the Directive" (p. 120). Specifically, employees should not expect to have a right of access to every mention of their name in every memorandum through the files of their employer or companies that do business with their employer. "Officials agreed . . . . [but] [t]here was no consensus, . . . on how the problem should be analyzed as a legal matter under the Directive" (p. 120). As technology has changed, officials must now find some legal justification for exempting what was never intended to be covered. One response, which is not discussed in the book, has been the adoption of subsequent directives addressing specific technologies.[23] Perhaps another response would be to re-frame the Directive from a general prohibition to specifically target certain undesirable activities. For example, should the Directive be aimed against the *collecting* or *use*, rather than the *transferring* of certain kinds of "sensitive" information? Similarly, if the underlying concern is about "direct marketing," a much simpler regime could be created that merely prohibits direct marketing, or direct marketing without consent, in Europe. However, such a change in direction would be unexpected, because, according to the Europeans, "the regime is designed to protect important human rights" (p. 154).

One response that can be expected is limited enforcement. While this may not be satisfactory to the authors, it is consistent with the

---

23. *See* European Union Directive 98/10/EC of the European Parliament and of the Council, 1998 O.J. (L 101) 24 (on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment); European Union Directive 97/66/EC of the European Parliament and of the Council, 1998 O.J. (L 024) 1 (concerning the processing of personal data and the protection of privacy in the telecommunications sector).

European approach to regulation in general. As they point out, "[m]uch of the debate about the Directive comes down to a choice between broad laws, the European tendency, and narrow laws, the American tendency" (pp. 152–53). To say that "Europe cannot strictly enforce the letter of the Directive and at the same time announce that organizations can routinely ignore it," (p. 155), ignores the more cooperative approach to enforcement generally taken toward regulatory regimes in Europe, and undervalues the role of discretionary approach to enforcement that is taken both in Europe and the U.S. It also assumes that every aspect of the Directive should necessarily be made clear overnight. While this might be desirable, it does not reflect reality on either side of the Atlantic. American courts routinely announce new rules without specifying every detail of how they will apply.[24] Similarly, when a new statutory regime is enacted in the United States, often the regulatory agency administering it goes through several phases of rule-making before a final regime is in place. Further, the police do not always arrest nor do district attorneys always prosecute. This is especially true in Europe where "[d]iscretion is the stuff of the law."[25] Law is a last resort and "the formal process of prosecution [is] a kind of *eminence grise*, a shadowy entity lurking off-stage, often invoked, however discretely, yet rarely revealed . . . . [Regulators] must display patience and tolerance, rather than legal authority, for their goal is not to punish but to secure change."[26] Whereas the American regulatory model tends to be one of confrontation, the European model is cooperation.

Thus, although the sector-by-sector analysis of the potential impact of the Directive based on a literal reading found in Chapter 3 was insightful, it was not particularly realistic. As the authors acknowledge, there are not likely to be any seizures of laptop computers at the border, just because they might be contain personal data.[27] This explains much of the objection to their literal reading of the Directive and their analysis of laptops that the authors reported receiving as responses to their interim report on the book (p. 46, 70). Instead, enforcement action is

---

24. *See, e.g.*, Li v. Yellow Cab Co. of California, 532 P.2d 1226 (Cal. 1975) ("Our decision in this case is to viewed as a first step in what we deem to be a proper and just direction, not as a compendium containing the answers to all questions that may be expected to arise.").

25. KEITH HAWKINS, ENVIRONMENT AND ENFORCEMENT: REGULATION AND THE SOCIAL DEFINITION OF POLLUTION xiv (1984).

26. *Id.* at 191, 197.

27. That being said, the authors do report that a laptop containing sensitive medical information was seized at an airport under Sweden's data protection law (p. 72).

more likely to be taken against grievous offenders.[28] While it is helpful to know the potential reach of the directive, it would be more useful to know how similar privacy laws are currently enforced in Europe. As the authors discuss, "[t]he pattern in European data protection law has often been to announce strict rules that appear to prohibit desirable practices but to have considerably more flexibility in practice" (p. 162). Further, although occasional reference is made to existing privacy laws, they are not presented with the clarity that the authors used in Chapters 3–7 to lay out potential impacts of the Directive. This is particularly surprising since enforcement will be brought under the various national laws, not the Directive itself (p. 45). In reality there will not be one Directive, but a dozen privacy regimes with varying nuances. A clearer articulation of how current regimes have been implemented would give readers a better notion of how likely and to what extent enforcement will occur. The fact that existing regimes have not resulted in draconian enforcement is an indicator of what to expect in the future.

IV. PROTECTIONISM AND TRADE WARS

Although "no European official wishes to create a major trade war or prohibit practices that are desirable or vital to European and other economies" (p. 154), such could be potential effects of the new Directive. "As many senior EU officials have stated, the political will of Europe should not be doubted in this matter. Access to the enormous EU market will depend on compliance with data protection laws" (p. 154). Some have suggested that data protection laws could be used to serve economic protectionist goals. Swire and Litan discuss the potential protectionist effects of the Directive and how the World Trade Organization (WTO) could be called in to resolve disputes.

From the European perspective, the principle benefit on the restriction on data transfers would be the protection of individuals' privacy. However, a second benefit could also be the economic "protectionist advantage the restrictions would provide against competition from the United States and other countries" (p. 145). The authors distinguish two types of protectionist effects — the first is where companies based in Europe gain business at the expense of firms based in a third country. "For instance, suppose that a company in the United States finds it too expensive to comply with the Directive . . . . In this event a European firm might win business that otherwise would

---

28. *Cf.* HAWKINS, *supra* note 25.

have gone to the U.S. firm" (p. 145). A second fruit of protectionism is if a business based in a third country decides to move operations to Europe. One could envision a scenario in which "data processing and associated jobs shift from the United States to Europe" (p. 145).

Realistically, however, Europeans are more likely to be burdened by strict enforcement of the Directive than benefit from it. The costs of imports are likely to rise (p. 146). Many international businesses will either not conduct operations in Europe, or will be forced to run their European ventures as a separate business. Similarly, a company based in Europe "cannot run its U.S. or other third-country operations as part of the company" (p. 146). Europe could effectively become an island in an ocean of commerce. Further, "there is also the possibility that strict data protection rules in Europe, coupled with less strict rules in other countries, will pose a competitive disadvantage for Europe. The risk is that Europe will fall behind in creating the information society" (p. 151). This competitive disadvantage could give Europe further incentive to raise trade barriers to protect European businesses and firms, much as the United States was accused of doing regarding environmental standards.

As the authors suggest, these dynamic effects could lead to a showdown over privacy at the WTO. "Data protection laws at the national or EU level may violate the free trade rules administered by the World Trade Organization" (p. 189). This would occur were Europe to give permission for data transfers to one country but not to another similarly situated country. Under the General Agreement on Trade in Services (GATS), EU countries must give 'national treatment' to non-EU countries. Essentially a "company should not be put at a disadvantage solely because it is not from the importing nation" (p. 190), and should be treated as if it was a company of the importing nation. While GATS allows exceptions for data protection, these exceptions are limited (p. 191). Arbitrary or unjustifiable discrimination or a disguised restriction on trade in services would void the GATS exception. Europeans could argue that information is not being handled the same way in third countries because of an absence of a legal regime to prevent abuses. However, the authors report "considerable skepticism" from trade experts as to whether such a European position would survive WTO scrutiny (pp. 191–92). The difficulties of policing the regime will bolster a third country's case that enforcement was arbitrary or discriminatory. An American WTO claim would be even stronger if Europe allowed transfers to other countries that have weaker data protection regimes (p. 192). Thus it is clear that Europe will not be able to single-out and discipline the United States into enacting a data

protection regime. The choice for the EU will be all or nothing. This may present a case study opportunity to see how the European Union really functions. How will member nations respond? Will the EU be willing to confront the United States on this issue?

At the heart of the controversy over enacting a privacy regime is a classic debate between use of the market and use of regulations to achieve policy objectives. Opponents of the regime argue that consumers will discipline data users if they fail to provide adequate privacy protections. Proponents contend that the market inefficiencies can only be corrected through a legal regime. In order to prevent a trade war or the potential invalidation of the entire privacy regime through a WTO ruling, the EU will need to accept a compromise solution in which the market drives non-EU businesses to adopt self-regulatory measures if they wish to compete in Europe. Approval of SRM contracts (essentially agreements by data users to provide "adequate" privacy protection through self-regulated means) provides businesses with the assurance that they need not fear legal prosecution as long at they adhere to their internal practices, and helps insulate the EU from challenges in the WTO for discriminatory treatment against those who process data outside of Europe (p. 193). As the authors note, the "threat of a WTO claim thus presents an important additional reason for European authorities to find ways to accommodate self-regulatory measures where adequate protection exists" (p. 196).

One decision under the Directive that will help avert a trade war is that "transfers after October 1998 will *not* need to be approved in advance by data protection authorities" (p. 158). This will prevent the kind of disruption in trade that would lead to an immediate claim before the WTO. In order to further avoid such claims, European officials will have to act quickly to articulate how adequacy will be determined. "We have yet to learn much in practice about how findings of inadequacy will be made" (pp. 44–45). The delineation of such a process will hopefully reduce apprehension about the Directive. In contrast, a finding of U.S. inadequacy before any general standards were promulgated could lead to serious political difficulties and spark a trade war or drawn-out proceedings before the WTO. Europe has every incentive to tread lightly and to use SRMs to achieve their goals. In this respect, the greatest value of the Directive may ultimately prove to be as a set of guiding principles for entities involved in exporting data from Europe rather than as a legal regime.

V. POLICY RECOMMENDATIONS

None of Your Business provides the reader on both sides of the Atlantic a rich selection of policy recommendations to consider. Well-thought through, these recommendations will help avoid potential conflict while giving the Directive meaningful scope. While most of the book is descriptive, these recommendations are prescriptive and represent a meaningful contribution to the debate over privacy protection. The recommendations are essentially broken into four categories: Self-Regulatory Measures for Private Actors, Recommendations for the European Union, Recommendations for the United States, and Recommendations for the Role of the WTO in Privacy.

A. Self-Regulatory Measures for Private Actors

Organizations in Europe and in third countries, including the United States, face many uncertainties about what data processing is permitted within the European Union (pp. 156–57). "To reduce these uncertainties, we strongly recommend that the organizations involved in significant transfers to third countries consider adopting self-regulatory mechanisms to govern such transfers" (p. 157). One advantage of SRMs is that they enable organizations that wish to comply with the Directive to do so, without waiting for a national legislature to pass a comprehensive privacy law or a data protection agency to begin an enforcement action. Such SRMs "must provide significant privacy protections that are adequate, but transfers should not be considered illegal simply because protections are not the same as in Europe" (p. 159). The authors predict that the success of SRMs may depend on finding a mechanism to ensure enforceability or to assure regulators that there will be a good level of compliance (pp. 159–61). Some form of sanctions or external verification would assist in this endeavor (p. 161). Such contractual arrangements have been adopted within Europe, prior to the Directive. For example, the Italian-based company Fiat, signed a contract with its French subsidiary that obligated Fiat-Italy to offer the protection of French law to information transferred from Fiat-France to Italy.[29] SRMs should be drafted to allow the same flexibility of treatment to third country companies as

---

29. *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 492 (1995).

accorded to European companies (p. 163). Models for companies seeking to protect data privacy include the protection of trade secrets (p. 165). "In summary, companies might agree to follow certain policies and procedures as part of their compliance with data protection rules" (p. 167).

B. Recommendations for the European Union

The authors urge European officials to recognize those sectors of the U.S. economy in which protection is adequate. "Some sectors do have significant privacy legislation and can make an especially strong case for the existence of adequate protection. Notable examples include individual credit histories, telephone records, student records, U.S. government records under the Privacy Act, communications governed by the Electronic Communication Privacy Act, cable television records, and video rental records" (p. 172). For those areas in which U.S. legislative protections are not deemed adequate, the authors "strongly recommend that EU countries find that [SRMs and contractual] measures, when properly drafted, constitute adequate safeguards of privacy under Article 26(2), so that compliance with them would protect would protect a company from enforcement actions" (p. 157). To that end, the authors were pleased to note that European officials are "noticeably more open to the use of contracts than [they] appeared to be in . . . 1997" (p. 163). "As it has become more clear to the Europeans that the United States and other countries will not pass comprehensive privacy laws, European officials have become more willing to find workable contract and other SRM solutions. . . . Because of the reality that significant and desirable data flows to third countries will otherwise not comply with the Directive, it is of great practical importance to arrive at a sensible policy on model contracts and other SRMs" (p. 173).

In a unique contribution to the general debate over privacy protection, Swire and Litan propose distinguishing between data regarding people in their individual capacity and data bout them in their business capacity (pp. 118–21). Although the two sorts of information are treated the same under the text of the Directive, the authors express "substantial doubt whether information concerning a person's business activities warrants the same strict level of protection as more clearly personal information" (p. 71, n.22). This distinction between the "business persona" and the "private persona" comports well with Justice Brandeis's conceptualization of privacy as the "right to be let

alone."[30] Obviously, one engaging in commerce does not have the same expectation of privacy regarding this activity as something they do with their family or alone. Engaging in commerce necessarily involves some degree of waiving the "right to be let alone." Therefore it is appropriate to apply different rules to information gathered or processed about individuals in their business capacity. In addition, "the risk to privacy interests is lower" in the business context (p. 119). The authors offer the example of gathering a list of participants at a business meeting, or the names of purchasing agents for business-to-business sales. In a business capacity individuals often want to make contacts and be included in a customer's database. However, none of the exceptions under the Directive would permit such activities without a showing of "adequacy" or significant hassle — such as asking every individual who gave a business card permission to include their name in a database. Although one might think such permission would be implied by the giving of a business card, the "unambiguous consent" language of the Directive would not allow such an assumption. Clearly "[a]pplying strict data protection rules to the vast range of business-to-business transactions, which only incidentally include named information, would be an enormous regulatory effort only distantly related to the core concerns of privacy protection" and would prohibit largely desirable activities (p. 119).

The Directive is largely aimed at protecting the individual against large data processing entities, such as corporations. As a result, less protection is needed for businesses, which through sheer size, are better equipped to take care of themselves. "[C]ompanies already have a strong business incentive, without the need of data protection laws, to protect against disclosure of commercially valuable or embarrassing information" (p. 119). Thus, "it likely makes sense to have fewer data protection restrictions on information that is processed about individuals in their business capacity" (p. 119). The authors suggest that EU officials use the determination of adequacy "in the light of all the circumstances"[31] in order to distinguish between data regarding the "business persona" and the "private persona" (p. 120). The circumstances would include whether data processing was about a person's business capacity. If so, then the level of protection required to achieve "adequacy" would be lower. Alternatively, information about

---

30. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

31. European Union Directive 95/46/EC, *supra* note 1, at art. 25(2).

a person, which is processed because of a decision concerning her employer, could be treated as information about that employer. Since most European countries do not subject information about companies to data protection rules, this would remove "business persona" data from the scope of the Directive (p. 119). Treating data about an individual in their business capacity as distinct from that in the individual capacity will allow both data users and EU officials to focus on the activities "that pose the greatest threats to privacy" (p. 167).

C. Recommendations for the United States

Swire and Litan acknowledge that there are important similarities between the privacy regimes in Europe and the United States, and that even where American privacy laws fail to provide remedies for certain violations, private tort and contract remedies may be available (p. 177). They do not recommend the adoption of a privacy regime such as the European privacy Directive, which "[t]o American sensibilities . . . might easily seem an unnecessary regulatory intrusion into how an organization should manage its own information" (p. 178). Their principal recommendation is for the creation of a "more structured institutional home within the U.S. government to consider issues arising from the private sector use of personal information" (p. 178). This home would be an "Office of Electronic Commerce and Privacy Policy" ("OECPP") that would make and coordinate policy with respect to privacy and electronic commerce, but that would not be a regulatory or enforcement agency (p. 179). The lack of regulatory or enforcement powers by such an office is in keeping with the historical scope and mission of the Department of Commerce (p. 188). Such an office, housed within the Department of Commerce, would develop expertise on issues of electronic commerce and privacy and make this expertise available to state and federal lawmakers, businesses, and private citizens (p. 181). In addition, this office would provide someone to represent American interests at the international table when electronic business and privacy issues are discussed and provide a continuing contact for our international partners on these issues (p. 182–83). As privacy is but one source of conflict that is likely to arise from this new electronically interconnected era, such an office would also serve as a lightning rod for discussion of new issues as they arise.

D. Recommendations for the Role of the WTO in Privacy

The United States and other non-EU countries may challenge the Directive as an improper extraterritorial enactment and as serving protectionist goals. As discussed in Part IV, a challenge of protectionism could be brought before the World Trade Organization under the General Agreement on Trade in Services. Clinton administration officials have said "[i]f we have to go to the WTO, we will" (p. 189). Therefore, the WTO will likely be implicated in negotiations regarding privacy laws. "In this way the WTO might become a useful forum for resolving disagreements about data protection rules" (p. 189). Swire and Litan's discussion of the WTO role in a challenge to the Directive under the guise of protectionism was analyzed in Part IV; however, the authors also suggest that the "WTO could also provide an international forum for harmonizing the legal treatment of privacy protection" (p. 194). Nonetheless, they urge caution in using the WTO as such a forum. "[N]egotiations in the WTO are . . . hard to predict . . . . [and] could result in a more law-centered emphasis than the United States, with its emphasis on self-regulation, would prefer" (p. 195). Further, it will be difficult to expand the scope of the WTO into "complex issues such as privacy protection that are only modestly related to free trade and protectionism" (p. 196). As an example, the authors point out that "environmental concerns have been difficult to accommodate within the WTO framework" (p. 195). Thus, while "discussions in the WTO are probably one helpful way to address privacy issues," the authors urge caution, particularly against implementing "binding international rules, administered through the WTO" (p. 196).

VI. SHADOWS OF THE FUTURE: TRANSNATIONAL INTERNET CONFLICTS

Swire and Litan astutely recognize that the debate over privacy protection is but the first of many transnational conflicts that will arise from global electronic interconnection. The closing chapter of *None of Your Business* is dedicated to exploring "broader implications . . . for the future of the Internet, electronic commerce, and world data flows" (p. 197).

> In many ways, the most significant legal effect of the Internet will be that individuals, far more than before, will gain information and buy goods from other

> countries. Legal conflicts will arise concerning not only the misuse of private information but also the availability of pornography or gambling, consumer protection issues in international commerce, and many other areas where citizens of one country can suffer harm because of Web sites in other countries (p. 20).

American courts have already begun to struggle with this issue with respect to determining regulatory scope and proper jurisdiction. As one court noted, "[t]he unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet."[32] Countries and individuals alike may be forced to recognize that there are limits to national sovereignty and the reach of laws. This is not a new idea, particularly in a federal system such as the United States where 51 sovereign governments operate. "For many modern transactions, multiple sovereigns will have personal jurisdiction based on the significant activity within their borders. Consequently, even where jurisdiction exists, there is the additional important question of determining when a sovereign will impose its own rule, or instead choose to have the law of a different sovereign govern."[33] Such conflicts in American jurisdictions are resolved in part by the Supremacy Clause of the United States Constitution,[34] by the *Erie* doctrine,[35] and by states' choice of law rules, but this system has taken generations to develop.[36] Further, it is evident from the American reaction to the privacy Directive that a supranational solution would be difficult to obtain and implement. Even if such a solution were possible, the authors warn that "[i]t is particularly risky to impose supranational solutions for areas such as the Internet that are experiencing rapid

---

32. American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168–69 (1997) (holding that a New York statute making it a crime to use a computer to disseminate obscene material to minors violated the Commerce Clause).

33. Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW 991, 992 (1998).

34. U.S. CONST. art. VI, cl. 2.

35. *See* Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938).

36. Consider that the evolution of the *Erie* doctrine from Swift v. Tyson, 41 U.S. 1 (1841), through Hanna v. Plumer, 380 U.S. 460 (1965), took over 100 years and is still not entirely settled.

technological change" (p. 205). As discussed in Part III, bright legislative ideas can be quickly undercut by rapid technology change because there "are steep learning curves for both technology and its regulation" (p. 206).

How then does one police the Internet? One solution discussed by the authors is international arbitration. However, they note that there is no significant history of such arbitration involving a consumer's dispute with a merchant (p. 198). Nonetheless, "one might achieve an ex ante agreement to [Virtual Magistrate] dispute resolution (VMDR) in cyberspace. An agreement to VMDR would then be a condition of access to the net through a participating access provider. This condition would track the contractual terms in real world agreements, providing, for example, that 'all disputes arising out of or related to the contract shall be resolved by arbitration.'"[37] Credit card companies can also serve an arbitrator or insurer's role in resolving international consumer disputes (p. 210).

Swire and Litan suggest that difficulties of enforcement of international business agreements or policing international electronic commerce, including that on the Internet, will ultimately turn on whether the party in dispute is an "elephant" or a "mouse" (pp. 200–04). "Elephants are large, powerful, and practically impossible to hide," such as transnational corporations (p. 200). In contrast, mice are "small, nimble, and breed annoyingly quickly" such as fly-by-night Internet companies (p. 201). Thus the authors expect that, in conflicts under the Directive, large corporate operators of mainframe computers are likely targets for enforcement. However, as the authors also point out, large transnational corporations are also favorable candidates for self-regulatory measures. This is due not only to their size and structure, but also the external pressures they face from media attention and public interest groups. Thus they conclude that there is "more of a similarity between binding national laws and self-regulatory efforts than has usually been recognized. Under either approach, the largest companies are subject to particular pressure to comply" (p. 205). In contrast, they also conclude that "it will be extremely difficult for national regulators to effectively govern data processing by the mice of the electronic world" (p. 202). This would also be true of other areas of contention, such as consumer protection and intellectual property in which transnational conflict from electronic commerce can be expected (p. 199). Possible approaches include the use of arbitration and

---

37. Jack Goldsmith & Lawrence Lessig, *Grounding the Virtual Magistrate* (visited Apr. 15, 1999) <http://www.law.vill.edu/ncair/disres/groundvm.htm>.

insurance, as discussed above. The authors also note that a "buyer's club model can potentially reduce the risks of electronic commerce" (p. 208). There is clearly no easy answer, and the problems will only multiply.

VII. CONCLUSION

Swire and Litan conclude that "[t]he Internet presents new problems about how nations will coexist in an interdependent world" (p. 212) and the "privacy debate is a precursor of the sorts of debates we can expect about . . . other electronic commerce issues" (p. 207). Both observations are profound and true. Perhaps the expected conflict over the European privacy Directive will not amount to more than a war of words. Or perhaps, once the so-called "Y2K" computer problem is a distant memory and the common currency is in place, the European Union will exercise its political and economic muscle to force privacy offenders into compliance. Either way, Swire and Litan have supplied insightful policy suggestions that actors on both sides of the Atlantic should consider. Further, they have provided a timely discourse that raises significant questions about privacy expectations at a time in which the Internet is maturing, Web-based commerce is growing, and Internet-based companies are gaining legitimacy. *None of Your Business* tracks the legal confrontations and difficulties that necessarily emerge from electronic globalization. As the authors note, "[t]he challenge is to find a way between the global and the local" (p. 212). And that *is* our business.

John C. O'Quinn