HOUSTON LAW REVIEW

ARTICLE

E-COMMERCE AND TRANS-ATLANTIC PRIVACY

*Joel R. Reidenberg**

TABLE OF CONTENTS

* © Joel Reidenberg 2001. Professor of Law, Fordham University School of Law. An earlier draft of this paper was prepared for the "E-commerce and Privacy" Santa Fe Conference of the Institute for Intellectual Property & Information Law at University of Houston Law Center, May 31–June 2, 2001. I would like to thank Craig Joyce, Paul Janicke, and Ray Nimmer for organizing a tremendous workshop, and each of the participants for their most valuable insights. Portions of the text used in this Article were presented in my testimony before a U.S. House of Representatives Subcommittee. *See The EU Data Protection Directive: Implications for the U.S. Privacy: Hearing Before the Subcomm. On Commerce, Trade, and Consumer Protection of the House Comm. On Energy and Commerce,* 107th Cong.,. 1st Sess. (March 8, 2000) http://energycommerce.house.gov/107/hearings/03082001Hearing49/print.htm.

For almost a decade, the United States and Europe have anticipated a clash over the protection of personal information.[1] Between the implementation in Europe of comprehensive legal protections pursuant to the directive on data protection[2] and the continued reliance on industry self-regulation in the United States,[3] trans-Atlantic privacy policies have been at odds with each other. The rapid growth in e-commerce is now sparking the long-anticipated trans-Atlantic privacy clash.

E-commerce highlights the more general societal uncertainty and debate over fair information practices. Online activity both generates and requires substantial databases of personal information.[4] Whether transactions are person-to-person, business-to-consumer, or business-to-business, the global growth and promise of e-commerce means that large quantities of personal information will move across national borders in the context of transaction processing. The digital privacy divide between Europe and the United States is an important obstacle that will cause significant conflict for e-commerce participants.

This Article will first look at the context of American e-commerce and the disjuncture between citizens' privacy and business practices. The Article will then turn to the international

---

1. *See* Symposium, *Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 IOWA L. REV. 445 (1995); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 2–3 (1998) (noting that the United States and Europe are on a "collision course" over the adequate protection of privacy).

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].

3. Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1318 (2000) ("The United States . . . has a market-dominated policy for the protection of personal information and only accords limited statutory and common law rights to information privacy.").

4. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1624, 1627, 1629 (1999) (noting the large amount of personal information generated from Internet use and that this information is shared and commercialized).

context and explore the adverse impact, on the status quo in the United States, of European data protection law as harmonized by *Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*[5] ("European Directive"). Following this analysis, the Article will show that the "safe harbor" agreement between the United States Department of Commerce and the European Commission[6]—designed to alleviate the threat of disruption in trans-Atlantic data flows and, in particular, to mollify concerns for the stability of online data transfers—is only a weak, seriously flawed solution for e-commerce. In the end, extra-legal technical measures and contractual mechanisms might minimize privacy conflicts for e-commerce transactions, but an international treaty is likely the only sustainable solution for long-term growth in trans-border commercial interchange.

I. E-COMMERCE AND U.S. DATA PROTECTION

E-commerce does not raise particularly new data privacy issues. E-commerce does, however, increase the level of complexity in dealing with the interests of citizens in the fair treatment of their personal information and with the commercial goals of transacting parties. There is also a qualitative change in the nature of data processing activity for e-commerce. Online commercial transactions depend on both the creation and availability of unprecedented and extensive data about individuals. At the same time, the boundary lines between sectors, and between offline and online data, are blurring. E-commerce, in effect, pushes a dramatic increase in the importance of data privacy issues for consumers, business, and society. But, United States policy lags far behind and, despite greater public attention, remains relatively stagnant with a culture of data stalking and information trafficking.[7]

---

5. Directive 95/46/EC, *supra* note 2.

6. Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 45,665–686 (July 24, 2000); Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7.

7. *Privacy and Electronic Communications: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. 52–53 (2000) [hereinafter *Hearing*] (statement of Joel R. Reidenberg, Professor of Law and Director of the Graduate Program, Fordham University School of Law) (noting that data stalking and information trafficking are normal practices in the United States and "legal rights . . . do not respond to abusive data practices").

A. Transactional Data and Profiles

E-commerce leaves an extensive trail of personal information. Internet service providers and Web sites log user interactions for technical and commercial operations.[8]

Online payment systems record basic details about the transacting parties and their transactions.[9] This information may be passed along to a variety of participants in the settlement of those transactions.[10] Over time, these data trails create rather intensive databases of personal information.[11]

The warehousing of transaction information and profiling of online users has become a key strategy in the business models of e-commerce companies.[12] Businesses believe they can better service customers and better target prospects if they analyze detailed behavioral information. Many of the prominent Internet-based companies such as Amazon, Yahoo, and DoubleClick started with business models that depended on advertising revenue.[13] Complex information sharing arrangements among online commercial Web sites—such as banner ad placement, cookies, or "phone home" software—that each transfer clickstream information to third parties become extremely important to business ventures. The behavioral information enables sites to categorize users and present them with content assumed to be of interest. In fact, as the technological capabilities become more sophisticated, the transfer of personal information is increasingly buried or hidden from users.[14]

---

8. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1199-1200 (1998).

9. *See* Reidenberg, *supra* note 3, at 1320 (noting that electronic payment systems record data about the transacting parties).

10. *Id*. at 1322-23 ("Data may be collected in one location, processed elsewhere, and stored yet at another site . . . [and] that multiple intermediaries have access to and may process data in transit.").

11. *Id*. at 1323-24 (discussing the phenomenon of "data creep," which subscribes to the school of thought that "more is better"—thus, companies are warehousing more seemingly innocuous and anonymous data to generate both demographic and detailed individual profiles).

12. *See id*. at 1324 ("The ease of collecting and storing personal information coupled with enhanced capability to use it create tremendous commercial pressures in favor of unanticipated or secondary uses…[and] generate additional value."); Schwartz, *supra* note 4, at 1627 n.114 (asserting the collection of personal information has "'enormous' financial value…[and is] the new currency of the digital economy.'" (quoting Edward C. Baig et al., *Privacy*, BUS. WK., Apr. 5, 1999, at 84)).

13. *See e.g.* Yahoo! Inc., Form 10-Q, at 16 (Sept. 30, 1998) ("successfully achieving our growth plan depends on … the successful sale of web-based advertising by our internal sales force." http://www.sec.gov/Archives/edgar/data/1011006/0001047469-98-040804.txt

14. For example, users needed a packet sniffer or personal firewall to discover the phone home features of Real Network's products and of the Microsoft smart download. *See* Brad King,

Transaction data and profiles are not limited to the online world. The blurring of borders between offline activities and online interactions creates significant information privacy concerns. DoubleClick and Alexa each sought to merge online information with the offline data to create more detailed dossiers of individuals.[15] Both faced lawsuits and public outrage.[16] In fact, the blurring of borders also extends to the public sector's use of private sector data. The FBI, for example, uses private databases.[17] Most likely, Congress could not, as a political matter, authorize the FBI to create the same database. More troubling, during the 2000 Presidential election thousands of Florida voters were excluded from the polls because ChoicePoint, a private company working for the state, inaccurately identified those individuals as convicted felons who were ineligible to vote.[18]

With the collapse of many start-up Internet companies, the disposition of transaction databases becomes a troubling problem.[19] Toysmart.com, an online toy store, was the unwitting pioneer in the conflict between bankruptcy and privacy.[20] The company's database was just another asset for sale in the liquidation, notwithstanding the privacy commitments made to users that no personal information would be transferred to third parties.[21] More recently, eTour.com ran into the same issue when the failing company sold its database to AskJeeves.[22] Between data warehousing, profiling, and bankruptcy asset liquidations,

---

File Tracker May Go Too Far (May 11, 2001) (describing stealth file tracking software), *at* http://www.wired.com/news/mp3/0,1285,43714,00.html.

15. *In re* DoubleClick, Inc. Privacy Litig., No. 00 CIV. 0641 NRB, 2001 WL 303744, at *5 (S.D.N.Y. Mar. 29, 2001).

16. *See id.* at *1 (stating the plaintiffs' federal and state law claims against DoubleClick); *Amazon Unit Settles Lawsuit* (Apr. 27, 2001), *at* http://www.siliconvalley.com/docs/news/tech/063587.htm.

17. Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask Choicepoint*, WALL ST. J., Apr. 13, 2001, at A1 ("[I]n the past several years, the FBI, the Internal Revenue Service and other agencies have started buying troves of personal data from the private sector.").

18. Gregory Palast, *Florida's Flawed "Voter Cleansing" Program*, *at* http://www.salon.com/politics/feature/2000/12/04/voter_file/index.html (Dec. 4, 2000).

19. *See* Walter M. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?* (((manuscript pp. 6–7))) 38 HOUS. L. REV. ____ (2001) (noting that bankruptcy trustees may be able to sell transaction data).

20. *See FTC Announces Settlement With Bankrupt Web Site, Toysmart.com, Regarding Alleged Privacy Policy Violations* (July 21, 2000), *at* http://www.ftc.gov/opa/2000/07/toysmart2.htm.

21. *Id.*

22. *See* Andrew Heavens & Stephanie Kirchgaessner, *Privacy Fears Over eTour Deal* (May 23, 2001) (discussing the sale of eTour.com's customer database), *at* http://news.ft.com/ft/gx.cgi.

American consumers perceive that they have lost control over their personal information.[23] For e-commerce, this belief becomes an obstacle to the growth of online transactions.[24]

B. Data Stalking and Information Trafficking in the United States

Sadly, the protection of personal information is a long-standing problem in the United States. In 1977, after three years of Congressionally mandated study, the U.S. Privacy Protection Study Commission, reported back to Congress that "neither law nor technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him."[25] Today, almost twenty-five years later, the Commission's conclusion remains equally true despite the rhetoric of self-regulation, technological mechanisms, and sectoral rights.

While there has been important progress in online privacy over the last few years, the state of Americans' data privacy nevertheless is appalling. Data stalking and information trafficking have become the norm in the United States.[26] As technical capabilities advance, commercial pressures enhance the tracking of citizens. Over the last two years, Americans have been horrified to learn of Intel's plan to impose a hidden digital fingerprint for the users of every Pentium III chip,[27] of Microsoft's equivalent to a digital social security number secretly emblazoned on files,[28] of DoubleClick's surprise plan to match offline data with hidden collections of online data,[29] and of

---

23. *See* Business Week/ Harris Poll: A Growing Threat, Business Week, March 20, 2000, at 96 [hereinafter *Business Week Poll*] (revealing consumer fears of privacy invasions online).

24. *See, e.g., Exposure in Cyberspace*, WALL ST. J., Mar. 21, 2001, at B1 (reporting, in a Wall Street Journal and Harris Interactive poll, that eighty-one percent of Americans refrained, at least "rarely," from using a Web site or making an online purchase due to privacy concerns).

25. THE REPORT OF THE PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 8 (1977).

26. *Hearing*, *supra* note 7, at 52 (statement of Joel R. Reidenberg).

27. *See Pentium III Processors: Processor Serial Number Questions & Answers* (describing the Intel processor serial number feature), *at* http://www.intel.com/support/processors/pentiumiii/psqa.htm (last visited July 11, 2001).

28. *See Junkbusters: Privacy Advisory on Microsoft Hardware IDs* (warning that "[f]iles produced by several popular Microsoft applications programs include a *fingerprint* or *tattoo*" that may identify a particular computer), *at* http://www.junkbusters.com/microsoft.html#history (last visited July 17, 2001).

29. *See* Letter from Joel Winston, Acting Assoc. Dir., Div. of Fin. Practices, Fed. Trade Comm'n, to Christine Varney, Counsel for DoubleClick, Inc. (Jan. 22, 2001) (discussing the FCC's investigation of DoubleClick's plan to merge offline and online data), *at* http://www.ftc.gov/os/closings/staff/doubleclick.pdf.

RealNetwork's surveillance of music listeners.[30] Despite these public scandals, even now, a popular version of Microsoft's Internet Explorer (Version 5.0) comes equipped with default settings that facilitate hidden surveillance of users, and a still widely used version of Netscape Communicator (Version 4.72) reports back to Netscape every time a user reads Messenger email. The next generation Internet transmission protocol may even force every device connected to the Internet to have the equivalent of a national identification number.[31] In effect, the tendency in the United States is to develop technology that increases data collection and decreases the transparency to citizens of such monitoring.

As a result of increased computing and communications power, previously unimaginable profiles of citizens are now readily available on the Internet. For example, Venture Direct, a New York based company, sells a list of heavy black women who are offered as targets for self-improvement products.[32] Not to be outdone, Acxiom, a company unknown to the public at large but holding dossiers on 160 million Americans, boasted of its "new ethnic system . . . identifying individuals who may speak their native language, but do not think in that manner."[33] Acxiom was essentially offering a list of ethnic Americans who "speak foreign," but "think American." Not surprisingly, within weeks of receiving publicity for this outrageous example at a meeting of the National Association of Attorneys General in September 1999, Acxiom removed its full data catalog from the company's Web site.[34] Now the site merely offers "specialty lists" with a specific mention of the Hispanic market[35] and declines to state clearly that those on the list can even learn of the existence of their profile.[36]

---

30. *See* Brian McWilliams, *Real Networks* [sic] *Hit With Privacy Lawsuit*, INTERNET NEWS, (Nov. 9, 1999) (discussing RealNetworks' practice of uploading information about their customers' listening habits), *at* http://www.internetnews.com/streaming-news/article/0,,8161_235141,00.html.

31. *See* John Markoff, *A Plan to Expand Internet Addresses*, N.Y. TIMES, May 14, 2001, at C10.

32. *See Venture Direct List* (advertising a list of subscribers to BELLE, The Magazine for Full-Figured Black Women), *at* http://www.venturedirect.com/scripts/index.php?script&&response&&list4416 (last visited July 12, 2001).

33. Acxiom Product Catalog, p. 5 (1999) (on file with author).

34. The author used Acxiom as an illustrative example at the meeting of state Attorneys General Privacy Task Force in September 1999. Acxiom's general counsel was also a participant at the meeting.

35. Acxiom, *Infobase Specialty Lists*, *at* http://www.acxiom.com/DisplayMain/0,1494,USA~en~938~976~0~0,00.html (last visited July 9, 2001).

36. *See* Acxiom, *Notice, Access, Choice* (stating that "Acxiom's policy does not allow non-public individual information to be provided directly to a consumer" but

These egregious practices in the business community are just a few examples that offend common decency and represent invidious stereotyping. Even for companies that try to engage in fair information practices, the threshold of acceptable conduct keeps rising. As the public and advocacy groups learn of new abuses, their expectations for fair treatment increase.

Nevertheless, industry lobbyists like to say that such abusive practices have not resulted in economic loss to individuals and that protection of privacy would be costly to society.[37] Lobbyists report astronomical costs to increase privacy for personal information,[38] but the methodology used to come up with many of these cost estimates is staggeringly specious.[39] Recent studies seem to start with the highest target the study authors think is politically correct and then seem to figure out how to get there. For example, one well publicized study "found" that privacy legislation for Web sites in the United States would cost between $9 and $36 billion.[40] Curiously, this particular study calculated the cost by asking a group of consultants how much they would charge to write software from scratch that would enable Web sites to provide data subject access.[41] The consultants were asked to assume the database contained Web site registration information on 100,000 to 10 million users and that the Web site already "allow[s] users to review and update their basic [information]."[42] The consultants estimated costs ranging from $44,000 to $670,000 per site![43] The study then used $100,000 per Web site to come up with its headline numbers.[44] Does anyone really believe that off-the-shelf products would not be developed at a fraction of this cost if data subject access were

---

also offering to "provide an individual with a copy of the non-public information" they maintain for a five dollar fee), *at* http://www.acxiom.com/DisplayMain/1,1494,USA~en~745~616~0~0,00.html (last visited July 12, 2001).

37. *See, e.g.*, ROBERT W. HAHN, AN ASSESSMENT OF THE COSTS OF PROPOSED ONLINE PRIVACY LEGISLATION 23–24 (May 7, 2001) ("[C]osts [of proposed laws to protect privacy] could be in the billions if not tens of billions of dollars."), *at* http://www.actonline.org/pubs/HahnStudy.pdf.

38. *See, e.g., id*; s*ee also* ONLINE PRIVACY ALLIANCE, *Resources* (providing links to recent studies on the economic impact of increasing the privacy of personal information), *at* http://www.privacyalliance.org/resources/research.shtml (last visited July 11, 2001).

39 See Robert Gellman, Why the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete, 20-24, Paper presented at the Ford Foundation Digital Media Forum, (June 2001); Peter Swire Home Page, http://www.osu.edu/units/law/swire.htm (last visited Sept. 23, 2001).

40. HAHN, *supra* note 37, at 23.

41. *Id.* at 16.

42. *Id.*

43. *Id.* at 20.

44. *Id.* at 21.

required? The study also assumed that small to medium sized Web sites would hire expensive outside consulting firms rather than high school computer whizzes to write software from scratch![45] Worse yet, the study ignored any financial losses attributable to weak privacy protections.[46] For example, Forrester Research reports that U.S. consumers spent $12 billion less online last year as a direct result of inadequate privacy protection.[47]

Even aside from a game of numbers, economic damage arguments seriously misconstrue the harm to society from the loss of faith and confidence in the fairness of information practices. Privacy is about the democratic fabric of society.[48] The very misuse of personal information is a harm to the individual citizen in democratic society that calls for redress.

Existing legal rights in the United States simply do not respond to abusive data practices and the need for sanctions against the misuse of personal information.[49] American law is sporadic, confused, and wholly inadequate to protect citizens in the face of privacy-invasive technical advances and pervasive online commercial surveillance. The principal statutes protecting Americans' privacy in the context of electronic communications have simply not kept pace with private sector information processing developments. The Electronic Communications Privacy Act of 1986,[50] the Telecommunications Act of 1996,[51] the Cable Communications Policy Act of 1984,[52] and the Video Privacy Protection Act of 1988[53] each contain narrow data privacy provisions that do not cover the vast array of online activities.[54] Indeed, Congress has granted drug abusers greater

45. HAHN, *supra* note 37, at 16.

46. *See id.* at 21–24 (declaring that online privacy legislation would be costly to the consumer without accounting for losses attributable to weak privacy protections).

47. *See* Paul Davidson, *Marketing Gurus Clash on Internet Privacy Rules*, USA TODAY, Apr. 27, 2001, at 1B.

48. *See* Reidenberg, *supra* note 3, at 1325 (noting that information privacy is recognized as a vital element of a civil society by democracies around the world); Schwartz, *supra* note 4, at 1653 (arguing that data privacy is necessary for democratic deliberation and individual self determination).

49. See PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 33–35 (1996) (discussing the limited reach of constitutional rights in protecting information privacy in the private sector).

50. 18 U.S.C §§ 2510–2522 (1994 & Supp. V 2000).

51. Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

52. 47 U.S.C. § 551 (1994 & Supp. V 2000).

53. 18 U.S.C. § 2710 (1994).

54. *See, e.g.*, *In re* DoubleClick, 2001 WL 303744, at *6-13 (S.D.N.Y. 2001) (discussing the difficulty of applying ECPA to online data sharing).

privacy protection than lawful users of the Internet.[55] Even the recent lawsuits filed across the country in several of the more prominent Internet data scandal cases are forced to rely on deceptive trade practice theories because basic privacy rights are not clearly established in either the common law or by statute.[56]

C. Self-Regulation and Technological Mechanisms to Protect Privacy

Despite the rising expectations of the American public for online privacy, policy decisions continually defer to industry self-regulation and technological mechanisms for fair information practices.[57] E-commerce proponents are strong advocates of the self-regulatory philosophy.[58] But the history of industry self-regulation and technological privacy demonstrate that these mechanisms have not and will not provide effective protection for citizens without the support of legal rights.[59] The non-regulatory solutions may have been promoted with the best intentions of industry and government policy-makers, but the conditions of market failure are too strong. In the end, self-regulation and technical tools have proven to be more public relations than meaningful information privacy for citizens. Indeed, as technology advances, so do public concerns and expectations for online privacy protections.

Yet, deeper than the practical experience of self-regulatory efforts, privacy rights mark the boundary between totalitarian and democratic governance. Privacy is central to our freedom of association and our ability to define ourselves in society.[60] These are basic political rights in a democracy and are fundamental American values. In contrast to the political nature of privacy, self-regulation assumes that all privacy values can and should be resolved by a marketplace. Democratic societies do not, however,

---

55. *Compare* 42 U.S.C. § 290dd-1 to -2 (1994 & Supp. V 2000) (imposing confidentiality of substance abuser's personal information), *with* 47 U.S.C. § 222 (Supp. V 2000) (making protections applicable only to service providers).

56. *See, e.g.*, *In re DoubleClick*, 2001 WL 303744, at *1 (relying on, inter alia, four state common law claims); McWilliams, *supra* note 30.

57. *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 774 (1999) ("[U.S. policy on] fair information practices has historically been predicated on the philosophy that self-regulation will accomplish the most meaningful protection of privacy without intrusive government interference and with the greatest flexibility for dynamically developing technologies.").

58. *Id.* at 775.

59. *Id.* at 773–81.

60. United States v. Citizens State Bank, 612 F.2d 1091, 1094 (8th Cir. 1980) (holding that "maintaining the privacy of one's associations may be necessary to guarantee freedom of association") (citing NAACP v. Alabama, 357 U.S. 449, 462 (1958).

typically sell off the political rights of citizens. Indeed, article 1, section 1 of the California state constitution was amended by referendum to include express protection for privacy and to apply that protection against businesses gathering and using personal information.[61]

Reliance on self-regulation is not an appropriate mechanism to achieve the protection of basic political rights. Self-regulation in the United States reduces privacy protection to an uncertain regime of notice and choice.[62] As a set of privacy principles, this approach misses key elements of the package of universally recognized fair information practice principles such as data minimization, data access, and storage limitations.[63] Self-regulation also enables data collectors to change the rules after the data has been collected from individuals.

As a practical matter, most Web privacy notices are nothing more than confusing nonsense for the average American citizen.[64] Policies are often found only through obscure links buried at the bottom of a Web page and are routinely made "subject to change." Once found, a linguistic analysis of the policies of ten major Web sites affected by data scandals shows that readers will not be able to understand the privacy statements without at least a college education and many could not be understood without a post-graduate education.[65] In fact, privacy policies are practically impossible to draft at a reading level most Americans can comprehend. Self-regulation, thus, denies the average American citizen an opportunity to make informed choices and reserves privacy for the nation's college educated citizens.

The Web seal programs are not a substitute for clear independent legal recourse. Seals, at best, offer an incomplete response to the misuse of personal information. Seal programs establish inconsistent substantive privacy standards for Web

---

61. *See generally* Hill v. NCAA, 865 P.2d 633 (Cal. 1994) (relying on the referendum ballot pamphlet in holding that constitutional protections apply against non-governmental organizations).

62. *See* NAT'L TELECOMM. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, ELEMENTS OF EFFECTIVE SELF-REGULATION FOR PROTECTION OF PRIVACY (Jan. 1998) (stating that, for self-regulation to be meaningful, businesses must adhere to substantive rules regarding notification and choice, rather than articulating broad policies or guidelines in these areas), *at* http://www.ntia.doc.gov/reports/privacydraft/198DFTPRIN.htm.

63. *See* Reidenberg, *supra* note 3, at 1325–29.

64. These notices parallel the problems faced by consumers in understanding the myriad of vaguely worded, but lengthy, privacy notices sent by conglomerate financial institutions pursuant to their Gramm-Leach-Bliley Act obligations. *See* 15 U.S.C. §§ 6801–6803 (Supp. V 2000).

65. *See* Will Rodger, *Privacy isn't Public Knowledge: Online Policies Spread Confusion with Legal Jargon*, USA TODAY, May 1, 2000, at 3D ("Every policy studied is written at a college level or higher.").

sites' use of personal information.[66] Programs such as TRUSTe omit key fair information practice standards from the minimum requirements of certification such as mandatory access to stored personal information.[67] With the rare exception of the Entertainment Software Rating Board (ESRB), seal programs do not require, as a condition for certification, that damage remedies be granted to the victims of information misuse.[68] Seal programs are also unlikely to cover the vast majority of Web sites. The two major seal programs, BBBOnline and TRUSTe, collectively certify a miniscule fraction of American Web sites.[69] Major sites such as Amazon.com do not even appear to participate.

Furthermore, seal programs narrowly restrict the scope of their certifications in ways that defy reasonable expectations of privacy. For example, TRUSTe only certifies sites with respect to the information that is "used to identify, contact, or locate a person."[70] Yet, Business Week reports that sixty-three percent of Internet users were uncomfortable with Web sites tracking their movements even though the sites did not tie the surveillance data with a user's name or real world identity.[71] Seal programs tend to apply only to the collection of data during specific, narrowly defined interactions such as those with Web sites. As a result, major data scandals involving TRUSTe licensees—such as Intel, Microsoft, and RealNetwork—turned out to be outside the scope of TRUSTe's certification.[72]

---

66. *Compare, e.g.*, *TRUSTe Program Principles* (requiring only that businesses offer users opt-out opportunities, encryption of personally identifiable information, and mechanisms for users to verify the accuracy of their personal information), *at* http://www.truste.com/programs/pub_principles.html (last visited July 22, 2001), *with BBBOnline: Privacy Program Eligibility Requirements* (including TRUSTe's program requirements in addition to requirements that the business does not share users' personal information with outside parties operating under a different privacy notice and that the business takes reasonable steps to assure that personal information is accurate, complete, and timely for the purpose for which it is used), *at* http://www.bbbonline.org/privacy/threshold.asp (last visited July 27, 2001).

67. *See TRUSTe Program Principles*, *supra* note 66.

68. *See ESRB Privacy Online Principles Guidelines and Definitions*, para. 6 ("If the participating company has not adhered to its privacy practices, consumers must be offered a remedy for the violations."), *at* http://www.esrb.org/wp_definitions.asp (last visited July 10, 2001).

69. *See Just Two Months After its One-Year Anniversary, BBBOnline Privacy Program Awards its 500th Seal* (May 9, 2000), *at* http://www.bbb.org/advertising/alerts/bbbolseal.asp; *TRUSTe Approves 1000th Web* Site (Jan. 12, 2000) (reporting on the 1000th seal approved by TRUSTe), *at* http://www.truste.com/about/about_1000th.html.

70. *TRUSTe Program Principles*,*supra* note 66.

71. *Business Week Poll*, *supra* note 23.

72. TRUSTe's program only covers data collected by a company's Web site from users. *TRUSTe Program Principles*, *supra* note 66. In the case of Intel, the microprocessor serial number was a hardware issue, the Microsoft Global Unique Identifier was a software issue, and the RealNetwork's phone home feature was also

Just as self-regulation and seal programs are flawed, the promise of technology does not work by itself. In a society in which the typical citizen cannot figure out how to program a VCR, how can we legitimately expect the American public to understand the privacy implications of dynamic HTML, Web bugs, cookies, and log files? The commercial models, however, are predicated on "personalization" and "customization" using these technologies.

Technologies are not policy neutral.[73] Technical decisions make privacy rules and, more often than not, these rules are privacy invasive. For technology to provide effective privacy protection, three conditions must be met: (1) technology respecting fair information practices must exist; (2) these technologies must be deployed; and (3) the implementation of these technologies must have a privacy protecting default configuration.[74]

The marketplace alone does not rise to meet these three conditions. One of the most celebrated technologies, P3P, has been on the drawing board since 1996.[75] Indeed, pressure from European legal requirements was instrumental in moving the standard forward and in affecting substantive privacy provisions. The standard, however, is still only a proposal. Even if the standard is finalized this year, P3P will be useless unless incorporated in Web browsers and widely adopted by Web sites.[76] And, even if P3P is incorporated in Web browsers and widely adopted by Web sites, the default configurations may still be set

---

a software tool. *Hearing*, *supra* note 7, at 52 (statement of Joel R. Reidenberg).

73. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 34–35 (1999) (noting that although "cookies" avoid the expense and inconvenience of passwords, their use is accompanied by the danger that a user's cookie file could be manipulated or copied to other systems, thus making them appropriate for use by sites, where little is at stake, but dangerous for granting access to databases securing sensitive information); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553, 571–72 (1998) (observing that the use of log files, which Internet browsers use to record the user's Web traffic patterns, can result in "substantive inalienable rules as a result of architectural decisions" because the recording protocol establishes a default rule for collecting personal data that a user can not change unless the architectural standards allow reconfiguration).

74. *See Hearing*, *supra* note 7, at 54 (statement of Joel R. Reidenberg).

75. *See Fed. Trade Comm'n: Public Workshop on Consumer Privacy on the Global Information Infrastructure*, official transcript, at 79–90 (June 4, 1996) (statement of Paul Resnick, Technical Staff, AT&T Infolab) (describing the then newly developed technology, PICS, the platform on which P3P would be built), *available at* http://www.ftc.gov/bcp/privacy/wkshp96/pw960604.pdf.

76. Microsoft has announced that it will incorporate P3P in the next version of Explorer. Glenn R. Simpson, *The Battle Over Web Privacy*, WALL ST. J., Mar. 21, 2001, at B1. But, Microsoft will, at best, be using an incomplete version of P3P, i.e. a P3P-Lite, because the final standard has not yet been adopted.

as a privacy-invasive implementation. Even if the default configurations are set to afford maximum privacy protection, P3P offers no means to assure that the practices of Web sites actually conform to stated standards. To paraphrase Justice Potter Stewart, "I do not know it when I cannot see it."[77]

Average citizens are in no position to make judgments about the impact of these technologies on their privacy. Despite widespread press reports about "cookies" technology and the routine deployment of this technology by Web sites to track site visitors, almost thirty percent of computer users still do not know about "cookies," and almost forty percent of computer users do not know how to de-activate them.[78]

In short, self-regulation and technology will not be adequate to ensure the public's right to privacy. With rising public expectations and increasing technical capabilities, the commercial environment becomes highly unstable. Seemingly innocuous data processing activity for an e-commerce participant may easily become the next front page privacy scandal. The complexity of e-commerce data-flows in a legal void guarantees continued public concern and conflict.

II. THE EUROPEAN CHALLENGES

Where online services suffer from a volatile environment of legal uncertainty in the United States, the situation in Europe is quite different. The European Directive on data protection takes another approach. The implications of the European legal approach for e-commerce and the United States are significant.

A. The EU Data Protection Directive

The background and underlying philosophy of the European Directive differs in important ways from that of the United States.[79] While there is a consensus among democratic states that information privacy is a critical element of civil society, the United States has, in recent years, left the

77. *See* Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (asserting, in Justice Stewart's famous words about pornography, "I know it when I see it").

78. *Exposure in Cyberspace*, WALL ST. J., Mar. 21, 2001, at B1 (reporting the results of a Wall Street Journal and Harris Interactive online survey).

79. *See generally* Reidenberg, *supra* note 3 (noting that, while Europe has a strong history of privacy legislation embodying first principles, the United States—despite its adoption of various privacy laws—has historically relied primarily on self-restraint for the implementation of data privacy standards).

protection of privacy to markets rather than law.[80] In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights.[81] European democracies approach information privacy from the perspective of social protection. In European democracies, public liberty derives from the community of individuals, and law is the fundamental basis to pursue norms of social and citizen protection.[82] This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop and in which information practices must serve individual identity. Citizen autonomy, in this view, effectively depends on a backdrop of legal rights. Law thus enshrines prophylactic protection through comprehensive rights and responsibilities. Indeed, citizens trust government more than the private sector with personal information.[83]

In this context, European democracies approach data protection as an element of public law. Since the 1970s, European countries have enacted comprehensive data privacy statutes.[84] Under the European approach, cross-sectoral legislation guarantees a broad set of rights to ensure the fair treatment of personal information and the protection of citizens. In general, European data protection laws define each citizen's basic legal right to "information self-determination."[85] This European premise of self-determination puts the citizen in control of the collection and use of personal information. The approach imposes responsibilities on data processors in connection with the acquisition, storage, use, and disclosure of personal information and, at the same time, accords citizens the right to consent to the processing of their personal information and the right to access stored personal data and have errors corrected.[86] Rather than accord pre-eminence to business interests, the European approach seeks to strike a balance and provide for a high level of protection for citizens.

As data protection laws proliferated across Europe during the 1980s, there were significant divergences among those laws, and harmonization became an important goal for Europe.[87] In

80. *Id.* at 1331.

81. *Id.* at 1347.

82. *Id.*

83. *Id.*

84. *Id.* at 1328.

85. *Id.* at 1326.

86. *Id.* at 1326–27 (listing Professor Colin Bennett's distillation of the First Principles of information privacy).

87. *See* JOEL R. REIDENERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND

1995, following the Maastricht Treaty of the European Union, the European Union adopted the European Directive[88] to harmonize the existing national laws within the European Union.[89] The European Directive sought to ensure that all Member States provided satisfactory privacy protection, and to ensure the free flow of personal information across Europe through the respect of basic, standardized protections.[90]

Under European Union law, a "directive" creates an obligation on each Member State to enact national legislation implementing standards that conform to those defined in the directive.[91] The European Directive requires that national law protect all information about an identified or identifiable individual whether or not the data is publicly available.[92] The European Directive also requires an individual's consent prior to processing personal information for purposes other than those contemplated by the original data collection.[93] The European Directive allows Member States to further restrict the processing of defined "sensitive" data—such as health information.[94] The European Directive restricts the collection and use of personal information not relevant for the stated purpose of processing.[95] The processing of personal information must be transparent with notice provided to individuals for the treatment of their personal information.[96] Organizations processing personal information must provide the data subjects with access to their personal information and must correct errors.[97] The European Directive

---

ONLINE SERVICES: REGULATORY RESPONSES 125 (discussing divergences in Member State law related specifically to online services).

88. Directive 95/46/EC, *supra* note 2.

89. Reidenberg, *supra* note 3, at 1329 ("Europe's goal is to harmonize fair information practices at a high level of protection.").

90. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446–52 (1995) (chronicling the Commission's desire to establish a regulatory scheme that would harmonize the already existing national laws adopted by the Member States).

91. Treaty Establishing the European Community, art. 249, *available at* http://europa.eu.int/eur-lex/en/treaties/dat/ec_cons_treaty_en.pdf (last visited Sept. 14, 2001).

92. Directive 95/46/EC, *supra* note 2, at arts. 2(a), 3, 4.

93. *Id.* at arts. 7(a), 14(b).

94. *Id.* at art. 8. For insightful discussions of the flaws in consent as a model of privacy protection, see the series of articles written by Paul Schwartz: *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 783–85 (2000); *Internet Privacy and the State*, 33 CONN. L. REV. 815, 821–23 (2000); and *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660 (1999).

95. Directive 95/46/EC, *supra* note 2, at art. 6(1)(c).

96. *Id.* at art. 10.

97. *Id.* at art. 12.

further requires that organizations maintain appropriate security for the processing of personal information.

For global information networks and electronic commerce, the comprehensive approach inevitably invokes some tension. Without the statutory authority to restrict transborder data flows, the balance of citizens' rights in Europe could easily be compromised by the circumvention of Europe for processing activities. Consequently, the European Directive includes two provisions to ensure that personal information of European origin will be governed by European standards. First, a choice of law clause in the European Directive assures that the standards of the local state apply to activities within its jurisdiction.[98] Second, a transborder data flow provision prohibits the transfer of personal information to countries that do not have "adequate" privacy protection.[99]

In terms of enforcement, each Member State must maintain an independent, national supervisory authority for oversight and enforcement of these privacy protections.[100] Significantly, the European Directive also mandates that Member State law require any person processing personal information to notify the national supervisory authority, which is required to keep a public register of data processors.[101]

The European Directive provided a transition period, ending in October 1998, for Member States to transpose these standards into national law.[102] However, as is not uncommon in the European system, nine Member States failed to comply strictly with the deadline.[103] By January 2000, the European Commission began proceedings before the European Court of Justice against France, Germany, Ireland, Luxembourg, and the Netherlands for their delays in transposition.[104] Although each of these countries had strong, existing data protection statutes, the European Commission argued that not all of the standards contained in the European Directive were satisfactorily addressed in their national laws. At present, proceedings before the European Court of Justice continue against France, Germany, and Luxembourg.

---

98. *Id.* at art. 4.

99. *Id.* at art. 25.

100. *Id.* art. 28(1).

101. *Id.* at arts. 18–19.

102. *Id.* at art. 31(1).

103. *Id.*

104. *Data Protection: Commission Takes Five Member States to Court, at* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/2k-10.htm (Jan. 11, 2000).

Notwithstanding the transposition delays, the harmonization achieved by the European Directive is significant, but does not remove all divergences among, and ambiguities in, European national laws.[105] By and large, the European Directive creates a strong baseline of protection across Europe. But small divergences and ambiguities will inevitably exist where the principles must be interpreted by different supervisory agencies in each of the Member States. These remaining divergences in standards can pose significant obstacles for the complex information processing arrangements that are typical in electronic commerce. For example, the European Directive requires that privacy rights attach to information about any "identifiable person."[106] Yet, the scope of this definition is not the same across the Member States; what some Member States consider "identifiable" others do not.[107] Similarly, the disclosures that must be made to individuals prior to data collection may still vary within Europe.[108] These differences can distort the ability and desirability of performing processing operations in various Member States because potentially conflicting requirements might apply to cross-border processing of personal information.

The effect of this challenge to comprehensive standards is, however, mitigated by consensus building options and extra-legal policy instruments that are available within the European system. The European Directive creates a "Working Party" of the Member States' national supervisory authorities.[109] The Working Party offers a formal channel for data protection officials to consult each other and to reach consensus on critical interpretive questions.

Compliance with the national laws has also been an issue in Europe. The notice and registration requirements, in particular, appear to have a spotty reception. One study conducted for the European Commission questioned whether data processors were adequately notifying their treatment of personal information to the national supervisory authorities,[110] and a recent study by Consumers International found that European Web sites were not routinely informing Web users of their use of personal

105. For an analysis of these divergences, *see* REIDENBERG & SCHWARTZ, *supra* note 88, at 125.

106. Directive 95/46/EC, *supra* note 2, at art. 2(a).

107. *See* REIDENBERG & SCHWARTZ, *supra* note 87, at 124–26.

108. *Id.* at 133–34.

109. Directive 95/46/EC, *supra* note 2, at art. 29.

110. *Existing Case-law on Compliance with Data Protection Laws and Principles in the Member States of the European Union*, Annex to the Annual Report 1998 of the Working Party Established by Article 29 of Directive 95/46/EC (Douwe Korff ed., 1998).

information.[111] Nonetheless, the existence of national laws and penalties does allow for enforcement actions in these cases of non-compliance.

B. Implications for the United States

The European Directive exerts significant pressure on U.S. information rights, practices, and policies. The Directive facilitates a single information market place within Europe through a harmonized set of rules, but also forces scrutiny of U.S. data privacy. In this context, the lack of legal protection for privacy in the United States threatens the flow of personal information from Europe to the United States. While business practices may offer privacy, and self-regulation may yield protections for personal information, the sheer complexity and confusion among such mechanisms becomes a handicap for data flows to the United States. At the same time, the European Directive is both having an important influence on privacy protection around the world and leaving Americans with legal protections as second class citizens in the global marketplace.[112]

Despite implementation divergences, the overall harmonization effect of the European Directive creates a common set of rules for the information market place in Europe. Companies operating within the European Union have the benefit of common standards across the Member States rather than fifteen diverse sets of conflicting national rules. This creates a large, level playing field for the treatment of personal information in Europe. With a high level of legal protection available on a cross-sectoral basis, Europeans do not face the same privacy obstacles for e-commerce that currently threaten the American experience. The culture of legal protection in Europe provides European companies with a competitive privacy advantage—when doing business in Europe—over the many American companies that are unaccustomed to applying fair information practices to personal information.

The European Directive also requires the national supervisory authority in each of the Member States and the European Commission to make comparisons between European

---

111. CONSUMERS INTERNATIONAL, *Privacy@Net: An International Comparative Study of Consumer Privacy on the Internet* 24 (Jan. 2001) ("Only a third (32.5%) of the sites that collected personal information and had a privacy policy bothered to alert the visitor to the privacy policy at the point where that information was collected.").

112. Countries from Asia to Latin America have followed the European comprehensive legal approach more closely than the American self-regulatory philosophy including Australia, Argentina, Canada, Hungary, and New Zealand. Refer to note 120 *infra* and accompanying text.

data protection principles and foreign standards of fair information practice.[113] The European Directive further requires that foreign standards of fair information practice be "adequate" in order to permit transfers of personal information to the foreign destination.[114]

For the United States, this means that both the national supervisory authorities and the European Commission must assess the level of protection offered in the United States to data of European origin. Because the United States lacks directly comparable, comprehensive data protection legislation, the assessment of "adequacy" is necessarily complex.[115] The European Commission and the national supervisory authorities recognize that the context of information processing must be considered to make any determination of "adequacy."[116]

Under the European Directive, the national data protection supervisory authorities and the European Commission must report to each other the non-European countries that do not provide adequate protection.[117] This bifurcated assessment of foreign standards means that intra-European politics can play a significant role in the evaluation of U.S. data practices. While a European level decision is supposed to apply in each Member State, the national supervisory authorities are independent agencies and will still have a degree of interpretive power over any individual case.

The end result for the United States, and for American companies, is that U.S. corporate information practices are under scrutiny in Europe and under threat of disruption when fair information processing standards are not applied to protect European data. Some commentators have predicted that any European export prohibition might spark a trade war that Europe could lose before the new World Trade Organization

113. Directive 95/46/EC, *supra* note 2, art. 25.

114. *Id.*

115. *See* First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy: Discussion Document of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, DG XV COM(97) D 5020 final, at para. 2 (June 26, 1997) (suggesting several criteria that should be met to meet the minimum standard of "adequacy" and noting the difficulties in applying standards to the United States and other countries without data protection legislation), *available at* http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp4en.htm; Preparation of a Methodology for Evaluating the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data, Annex to the Annual Report 1998 of the Working Party Established Under Article 29 of the Directive 95/46/EC, DG XV COM(98) D 5047, *available at* http://www.droit.fundp.ac.bc/crid/privacy/Tbdf/Chapitrel.pdf.

116. *Id.*

117. Directive 95/46/EC, *supra* note 2, at art. 25(3).

(WTO).[118] While such a situation is possible in theory, an adverse WTO ruling is unlikely.[119]

Even with the difficulties of the European approach, countries elsewhere are looking at the European Directive as the basic model for information privacy, and significant legislative movements toward European-style data protection exist in Canada, South America, and Eastern Europe.[120] This movement can be attributed partly to pressure from Europe and scrutiny of foreign privacy rights. But the movement is also due, in part, to the conceptual appeal of a comprehensive set of data protection standards in an increasingly interconnected environment of offline and online data. In effect, Europe, through the European Directive, has displaced the role that the United States held since the famous Warren and Brandeis article[121] in setting the global privacy agenda.

With the European Directive's imposition of both harmonized European legal requirements for the fair treatment of personal information and limitations on transborder data flows outside of Europe, U.S. companies recognize that they will have to respect European legal mandates.[122] Unless American companies doing business in Europe choose to flout European law, U.S. e-commerce businesses must provide stringent privacy

---

118. *See, e.g.*, SWIRE & LITAN, *supra* note 1, at 188–96.

119. *See, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 49–51 (2000) (explaining that the WTO would be very unlikely to rule for the United States in an action for the following reasons: (1) the EU Directive is facially applicable equally to all countries and companies; (2) the EU has a legitimate policy objective; and (3) prudential concerns).

120. *See, e.g.*, *Council of Europe, Chart of Signatories and Ratifications* ETS 108 (listing countries that have ratified the treaty on data privacy), *at* http://conventions.coe.int/ Treaty/EN (last visited July 10, 2000); INDUSTRY CANADA, THE INTERNATIONAL EVOLUTION OF DATA PROTECTION (justifying the Canadian proposal for a comprehensive privacy law by reference to the European initiative), *at* http://e-com.ic.gc.ca/english/fastfacts/43d10.htm (last modified Dec. 10, 2000); OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA, HONG KONG, PERSONAL DATA (PRIVACY) ORDINANCE, ch. 486 (showing that the Hong Kong statute follows European comprehensive model), http://www.pco.org.hk/english/ordinance/ordfull.html; HUNGARIAN REPUBLIC, THE FIRST THREE YEARS OF THE PARLIAMENTARY COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION 68–72 (1998) (discussing the influence of the European Directive for Hungarian data protection law); Pablo Palazzi, *Data Protection Materials in Latin American Countries* (detailing the emergence of data protection legislation in Latin America), *at* http://www.ulpiano.com/DataProtection-LA-links.htm (last modified Nov. 12, 2000).

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

122. *See* Shaffer, *supra* note 119, at 72–73 ("The timing of the multiple [privacy protection] efforts [by U.S. companies] in conjunction with the EU Directives coming in force in October 1998 is no coincidence.").

protections to data of European origin when processing that data in Europe or in the United States.

Concurrently, American law and practice allows those same companies to provide far less protection, if any, to data about American citizens. This is a particularly troubling aspect of U.S. opposition to the European Directive's standards. American companies will either provide Europeans with better protection than they provide to Americans, or they will treat Americans in accordance with the higher foreign standards and disadvantage those citizens doing business with local U.S. companies.

In effect, the proliferation of European-style data protection measures around the world increasingly means that American citizens will be left with second class privacy in the United States while being afforded greater privacy protection against American companies outside U.S. borders.

III. UNSAFE HARBORS

In response to the risk that Europe would block data flows to the United States and to great pressure from online industries, the U.S. Department of Commerce entered into negotiations with the European Commission to create a "safe harbor" agreement that would assure Europe of the adequacy of protection for data processed by U.S. businesses.[123] In the absence of statutory protection in the United States, the concept was that the European Commission would endorse a voluntary code of conduct that would meet the "adequacy" standard.[124] American businesses could then publicly commit to adhere to this code for the treatment of European origin data and be assured of uninterrupted data flows from Europe.

The lengthy and troubled negotiations on the code began in 1998 between the U.S. Department of Commerce and the European Commission.[125] Toward the end of the negotiations, some of the particularly difficult issues were: (1) the existence of a public commitment for companies adhering to the code; (2) the access rights; and (3) enforcement in the United States.[126] A final

123. *See* Letter from David L. Aaron, U.S. Dep't of Commerce, to Industry Representatives (Nov. 4, 1998), *at* http://www.ita.doc.gov/td/ ecom/aaron114.html.

124. *Id*.

125. *Id*.

126. *See* Letter from Robert S. LaRussa, Acting Under Secretary for Int'l Trade Admin., U.S. Dep't of Commerce, to John Mogg, Director, DG Internal Market, European Commission, (July 21, 2000) [hereinafter LaRussa Letter] (addressing final concerns of the European Commission with negotiations over a voluntary "safe harbor" and offering compromise by establishing a public list of companies that choose to adhere to the principles, agreeing that future U.S. data privacy legislation should apply to foreign

set of documents—including an exchange of letters, the Safe Harbor Privacy Principles, Frequently Asked Questions setting out interpretative understandings of the principles, and various annexes and representations made to the European Commission by the U.S. Department of Commerce and the Federal Trade Commission (collectively the "Safe Harbor")—was released in July 2000[127] and approved by the European Commission.[128]

While the approval was an important short-term political victory for both the United States and the European Commission, the Safe Harbor agreement is unworkable for both sides and will not alleviate the issues of weak American privacy protection. Indeed, choice of law issues may make Safe Harbor irrelevant for many e-commerce activities.

A. The Adoption of the "Safe Harbor"

1. The Political Dimension. For the European side, the United States posed a major problem. American law did not provide comparable protections to European standards, and fair information practices in the United States were rather spotty.[129] Yet, European regulators did not want to cause a disruption in international data flows.[130] The prospect of change in U.S. law seemed remote, and the European Commission would have serious political difficulty insisting on an enforcement action against data processing in the United States prior to the full implementation of the European Directive within the European Union. Similarly, while transposition remained incomplete, an aggressive enforcement strategy by a national supervisory authority could have hampered the national legislative debates on transposition. Safe Harbor offered a mechanism to delay facing tough decisions about international privacy and, in the meantime, hopefully advance U.S. privacy protections for European data.

On the U.S. side, the Department of Commerce faced strong pressure from the American business community to block the

---

transfers, and assuring the Commission that the agreement would do nothing to change jurisdiction), *at* http://www.export.gov/safeharbor/USLETTERFINAL1.htm.

127. Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 45,665–686 (Dep't Commerce, July 24, 2000) [hereinafter Safe Harbor].

128. Commission Decision, 2000/520/EC, 2000 O.J. (L 215) 7.

129. Refer to Part I *supra*.

130. *See* Shaffer, *supra* note 119, at 44–45 (noting the reluctance of EU officials to enforce the Directive's provisions during negotiations with the U.S. due to pressures from European businesses and the fact that the majority of the EU countries had not met the deadline for passing data privacy legislation).

European Directive.[131] The United States was not prepared to respond to the Directive with new privacy rights and wanted to prevent interruptions in transborder data flows.[132] Safe Harbor became a mechanism to avoid a showdown judgment on the status of American law and defer action against any American companies.

As such, the acceptance in July 2000 of Safe Harbor by the European Union was a transitory political success. At the national level in Europe, however, data protection agencies have expressed substantial opposition to Safe Harbor, and they will still have considerable latitude in dealing with the United States.[133]

2. The Dubious Legality of Safe Harbor. In the United States, however, Safe Harbor faces a serious jurisdictional obstacle to its enforcement—one of the key European criteria for acceptance. The U.S. Department of Commerce issued Safe Harbor documents "to foster, promote, and develop international commerce."[134] The agreement is predicated on the enforcement powers of the Federal Trade Commission under section 5 of the Federal Trade Commission Act.[135] Indeed, as part of the negotiations, the Federal Trade Commission represented to the European Commission that it would "give priority to referrals of non-compliance with safe harbor principles from EU member states."[136] Yet, the underlying legal authority of the FTC to enforce Safe Harbor is questionable.

As originally enacted by the Federal Trade Commission Act in 1914, section 5 applied only to unfair methods of competition.[137] Jurisdiction over "unfair or deceptive acts or practices" was extended to the FTC by the Wheeler-Lea Act of

131. *Id*. at 70–72.

132. *See id*. at 22–39 (explaining the historic and cultural preference for self-regulation over legislation to ensure data privacy in the United States and noting the enormous market pressure exerted by a threat to impede data European data flow).

133. *See, e.g.*, On the Level of Protection Provided by the "Safe Harbor Principles": Opinion of the Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, DG XV CA07 COM (00)434 final, [hereinafter Opinion of the Working Party] (objecting to the ambiguity of Safe Harbor, questioning the propriety of relying on the limited jurisdiction of the FTC to enforce the principles, and noting exceptions enumerated by Safe Harbor beyond the scope allowed by the European Directive), http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32en.htm.

134. LaRussa Letter, *supra* note 126.

135. 15 U.S.C. § 45(a) (1994).

136. Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n, to John Mogg, Director, DG XV, European Comm'n (July 14, 2000), http://www.export.gov/safeharbor/FTCLETTERFINAL.htm.

137. Fed. Trade Comm'n Act of 1914, ch. 311, § 5, 38 Stat. 719, 719 (1938).

1938.[138] The stated Congressional purpose was to enable the FTC to "restrain unfair and deceptive acts and practices which deceive and defraud the public generally."[139] Indeed, contrary to the purpose of Safe Harbor protecting U.S. business interests in international trade, the Wheeler-Lea Act amendments sought to protect the general public from unscrupulous business practices. In fact, at the time of the enactment of section 5, the FTC's jurisdiction expressly excluded foreign commerce, not to mention the protection of foreign consumers as envisioned by Safe Harbor.[140]

While the McGuire Resale Price Maintenance Act of 1952[141] expanded FTC jurisdiction into foreign commerce with respect to monopolistic pricing, the U.S. Supreme Court had specifically held that only Congressional amendments could expand the scope of the FTC's authority under section 5.[142] In *FTC v. Bunte Brothers*, the Commission unsuccessfully sought an expansion of its interstate commerce authority in the context of antitrust enforcement.[143] Congress eventually responded with the Magnuson-Moss Warranty—Federal Trade Commission Improvement Act of 1975[144] that was, according to the Senate Conference Report, designed "to improve its [the FTC's] consumer protection activities."[145] The 1975 amendments extended the jurisdiction to acts and practices "in or affecting commerce," but at no time contemplated protecting American business interests or foreign consumers.[146]

Hence, the assertion by the U.S. Department of Commerce and the FTC that Safe Harbor comes within the section 5 jurisdiction is a radical departure from the stated legislative purposes of the statute and in direct opposition to the Supreme Court's restrictive interpretation of section 5 authority.

Within Europe, the legality of Safe Harbor is also open to question. Under the European Directive, "adequacy" must be

---

138. Fed. Trade Comm'n Act Amendments (Wheeler-Lea Act) of 1938, 49, sec. 3, §5(a), 52 Stat. 111 (1938).

139. S. REP. CONF. NO. 221–1077.

140. 15 U.S.C. § 45(a).

141. Fed. Trade Comm'n Act Amendments (McGuire Resale Price Maintenance Act) of 1952, ch. 745, 66 Stat. 631, 632 (1952).

142. FTC v. Bunte Bros., 312 U.S. 349, 352–55 (1941) (holding that section 5 of the Federal Trade Commission Act did not give the FTC the authority to reach local commerce that affected interstate commerce without clear congressional authority).

143. *Id.* at 353–55.

144. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act of 1975, Pub. L. 93–637, § 201, 88 Stat. 2183, 2193 (1975).

145. S. CONF. REP. NO. 93–1408, at 1 (1974).

146. Pub. L. 93-637 § 201, 88 Stat. at 2193.

assessed in light of the prevailing "rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."[147] However, Safe Harbor was not yet in existence at the time of the approval by the European Commission. The European Parliament specifically noted this problem shortly before the approval by the European Commission.[148] Similarly, according to the European Directive, the European Commission only has authority to enter into negotiations to remedy the absence of "adequate" protection after a formal finding that the non-European country fails to provide "adequate" protection.[149] Yet, in the context of Safe Harbor negotiations, the European Commission never made a formal finding.[150] These would appear to be significant administrative law defects. Although the European Commission maintains that the European Parliament did not say that the Commission acted outside its powers, and the Member States voted unanimously in the political committee to accept Safe Harbor,[151] this administrative process problem remains an open question that only the European Court of Justice can resolve and gives the independent national supervisory authorities grounds to vitiate Safe Harbor through strict interpretations of the European Commission's ruling.

In addition, the European Parliament pointed out:

> [T]he risk that the exchange of letters between the Commission and the US Department of Commerce on the implementation of the 'safe harbour' principles could be interpreted by the European and/or United States judicial authorities as having the substance of an international agreement adopted in breach of Article 300 of the Treaty establishing the European Community and the requirement to seek Parliament's assent (Judgment of the Court of Justice of 9 August 1994: French Republic v. the Commission—Agreement between the Commission and the United States regarding the application of their competition laws (Case C-327/91)).[152]

147. Directive 95/46/EC, *supra* note 2, at art. 25(2).

148. EUR. PARL. DOC. (R5 305) 2 (2000).

149. Directive 95/46/EC, *supra* note 2, at art. 25(5).

150. The procedure for a formal finding is established in Directive 95/46/EC, *supra* note 2, at art. 25(4).

151. *See* Press Release, European Commission, Frits Bolkestein Tells Parliament Committee He Intends To Formally Approve "Safe Harbor" Arrangement With United States On Data Protection (July 13, 2000), *at* http://europa.eu.int/comm/internal_market/en/media/ dataprot/news/harbor5.htm.

152. EUR. PARL. DOC. (R5 305) 3 (2000).

B. The Limited Applicability and Increased Risks

Notwithstanding its validity in either legal system, the scope of Safe Harbor provision is very narrow. First, Safe Harbor by its terms can only apply to activities and U.S. organizations that fall within the regulatory jurisdiction of the FTC and the U.S. Department of Transportation.[153] As a result, many companies and sectors will be ineligible for Safe Harbor, including particularly the banking, telecommunications, and employment sectors that are expressly excluded from the FTC's jurisdiction.[154] Second, Safe Harbor will not apply to most organizations collecting data directly in Europe. Article 4 of the European Directive provides that, if a data controller is located outside of the European Union but uses equipment within the European Union, the law of the place where the equipment is located will be applicable.[155] This provision establishes a choice of law rule that greatly reduces the availability of Safe Harbor to international business. This provision of the Directive is especially significant in the context of Web-based businesses because interactive computing means that a European user will always make use of computing resources at the user's location. The courts of Member States, such as France, have shown in other areas a clear willingness to apply the substantive law of the place where an Internet user is located.[156] Hence, many cases, and particularly in the context of e-commerce, apply the substantive law of a Member State rather than Safe Harbor. The national data protection authorities have also endorsed this interpretation of the European Directive.[157]

By implication, Safe Harbor also raises the risks for data transfers by companies that do not subscribe to the code. The approval by the European Commission of Safe Harbor as an

---

153. Refer to notes 127-28 *supra* and accompanying text.

154. 15 U.S.C. § 45(a)(2) (1994); *see also* Safe Harbor, *supra* note 127, at 45, 675–78 (explaining limitations on FTC jurisdiction in these areas).

155. *See* Directive 95/46/EC, *supra* note 2, at art. 4. In fact, the translation of this provision creates a more liberal rule of jurisdiction in some countries where the term "means," rather than "equipment," is used. *See* REIDENBERG & SCHWARTZ, *supra* note 88, at 127–28.

156. *See, e.g.*, UEJF c. Yahoo!, TGI de Paris, Ord. en référé du 22 Nov. 2000; Joel R. Reidenberg, L'affaire Yahoo et la democratization internationale de l'Internet, Juris Classeur Communic. Commerce électronique, chron. 12 (May 2001).

157. Privacy on the Internet—An Integrated EU Approach to Online Data Protection: Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, DG XV COM (00)5063 final at 28 (noting the application of the substantive law of a Member State under Article 4 of the Directive in the context of cookies on hard drives in a Member State), http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf.

"adequate" basis to transfer personal information to the United States implicitly acknowledges that transfers outside the scope of Safe Harbor will not be adequately protected. Consequently, non-Safe Harbor transfers must be covered by one of the other exceptions to the transborder data flow rules, such as a transfer pursuant to a contractual arrangement.[158]

Ironically, Safe Harbor simplifies the task for national supervisory authorities to block data flows to the United States. The national agencies will readily be able to identify those U.S. companies that do not subscribe to Safe Harbor and have not presented a data protection contract for approval under the European Directive's Article 26 exceptions. In such cases, the presumption must be that the protection is "inadequate" and the data-flow must, under European law, be prohibited.[159]

Thus, for the United States Safe Harbor approach might compromise many U.S. businesses in a way that a legislative solution would not. For e-commerce, this risk is devastating.

C. Weakening of European Standards and Illusory Enforcement Mechanisms

For the national supervisory authorities in Europe, Safe Harbor poses a weakening of European standards.[160] In particular, the permissible derogations from Safe Harbor without a loss of coverage are significant. Safe Harbor exempts public record information despite its ordinary protection under European law.[161] Similarly, Safe Harbor exempts any processing pursuant to "conflicting obligations" or "explicit authorizations" in U.S. law, whether or not such processing would be permissible under European standards.[162] The access standard set out in Safe Harbor also includes derogations that do not exist in European law.[163]

Most importantly, however, Safe Harbor weakens European standards for redress of data privacy violations. Under the

158. Directive 95/46/EC, *supra* note 2, at art. 26. The European Commission has issued a model contract for this purpose. *See* http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clauses.htm (last visited July 14, 2001).

159. *See* Directive 95/46/EC, *supra* note 2, at art. 25.

160. Opinion of the Working Party, *supra* note 134 (noting the watering down of the Directive's standards under Safe Harbor due to exceptions for obligations under U.S. law, publicly available data, and other such loopholes, and recommending close monitoring of exception usage).

161. *Compare* Safe Harbor, *supra* note 127, at FAQ 8(7)–(8) (defining exemptions for publicly available data), *with* Directive 95/46/EC, *supra* note 2, at art. 2(a) (containing no exemption for such data).

162. *See* Safe Harbor, *supra* note 127, at 45, 667.

163. *See generally id.*

European Directive, victims must be able to seek legal recourse and have a damage remedy.[164] The U.S. Department of Commerce assured the European Commission that Safe Harbor and the U.S. legal system provided remedies for individual European victims of Safe Harbor violations.[165] The European Commission expressly relied on representations made by the U.S. Department of Commerce concerning available damages in American law.[166] The memorandum presented by the U.S. Department of Commerce to the European Commission, however, made misleading statements of U.S. law.[167] For example, the memorandum provides a lengthy discussion of the privacy torts and indicates that the torts would be available.[168] The memorandum failed to note that the applicability of these tort actions to data processing and information privacy has never been established by U.S. courts and is, at present, purely theoretical. Indeed, the memorandum cites the tort for misappropriation of a name or likeness as a viable damage remedy, but all three of the state courts that have addressed this tort in the context of data privacy have rejected it.[169] Safe Harbor is also predicated on dispute resolution through seal organizations such as TRUSTe.[170] Yet, only one seal organization, the ESRB, proposes any direct remedy to the victim of a breach of a privacy policy, and other organizations' membership lists look like a "Who's Who" of privacy scandal-plagued companies.[171]

Lastly, the enforcement provisions of Safe Harbor rely on the FTC.[172] Even if the FTC has jurisdiction to enforce Safe Harbor, the assertion that the FTC will give priority to European enforcement actions is hard to believe. First, although the FTC

---

164. Directive 95/46/EC, *supra* note 2, at arts. 22–23.

165. U.S. DEP'T OF COMMERCE, DAMAGES FOR BREACHES OF PRIVACY, LEGAL AUTHORIZATIONS AND MERGERS AND TAKEOVERS IN U.S. LAW (July 14, 2000) [hereinafter BREACHES OF PRIVACY], *available at* http://www.ita.gov/td/ecom/PRIVACYDAMAGESFINAL.htm.

166. Commission Decision 00/520/EC, art. 1(b), 2000 O.J. (L 215) 7, 8 (listing the memorandum as one of four documents the European Commission considered in determining Safe Harbor's adequacy).

167. BREACHES OF PRIVACY, *supra* note 165.

168. *Id*.

169. *See* Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995) (rejecting claim of breach of privacy against credit card company for renting information of cardholder's spending habits); Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975) (discussing magazine subscription lists); U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 WL 1065557 (Va. Cir. Ct. June 13, 1996) (stating the proposition that names do not have property value in the context of magazine subscription lists).

170. Safe Harbor, *supra* note 127, at 45,665–685.

171. Refer to Part I.C. *supra*.

172. Safe Harbor, *supra* note 127, at 45,668.

has become active in privacy issues recently, the agency's record of enforcing the Fair Credit Reporting Act, one of the country's most important fair information practices statutes, is less than aggressive. Second, were the FTC to devote its limited resources to the protection of Europeans' privacy, Americans should and would be offended that a U.S. government agency—charged with protecting American consumers—chose to commit its energies and U.S. taxpayer money to the protection of European privacy in the United States against U.S. businesses at a higher level than the FTC asserts for the protection of Americans' privacy.

Sadly, though, for many American companies even these weakened European standards impose substantially greater obligations than U.S. law. In particular, the notice, choice, access, and correction requirements are only sporadically found in U.S. law. As a result, pitifully few American companies have subscribed to Safe Harbor; indeed, as of June 21, 2001, fewer than fifty-five companies had signed up.[173]

The upshot of these sui generis standards, the unenthusiastic reception by American companies, and enforcement weaknesses is a likelihood that the national supervisory agencies will be dissatisfied with Safe Harbor and the Member States will face great political pressure to suspend Safe Harbor once transposition is completed. Thus, for e-commerce, the utility of Safe Harbor is rather dubious.

IV. AN INTERNATIONAL TREATY SOLUTION

With the trans-Atlantic divide on privacy so deeply entrenched, the United States is on the path to rapidly becoming the world's leading privacy rogue nation. Just a cursory examination of the data scandals over the last year and consumer privacy concerns for e-commerce suggest that our national policy of self-regulation will not work to assure public confidence and trust in the treatment of personal information, cannot work to guarantee citizens their political right to freedom of association and privacy, and will leave American businesses at a competitive disadvantage in the global information market place. At a time when Internet growth rates are greater outside the United States, and non-U.S. Web content is becoming an absolute majority of available Internet content,[174] United States

173. U.S. DEP'T OF COMMERCE, SAFE HARBOR LIST (reflecting only fifty-five subscribing company certifications), *at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited July 13, 2001).

174. *See, e.g., 55 Percent of All Web Traffic Worldwide Comes from Outside the United States*, STAT MARKET, http://statmarket.com/SM?c=stat012301 (Jan. 23, 2001).

interests are ill-served by avoiding the creation of clear legal privacy rights.

The United States desperately needs to establish a basic set of legal protections for privacy. Any such regulation must recognize that technologies will be essential to ensure privacy protections across divergent sets of rules in the global environment. In fact, technical decisions are not policy neutral. Technical decisions make privacy rules, and more often than not in the United States, these rules are privacy invasive. For technology to provide effective privacy protection, three conditions must be met: (1) technology respecting fair information practices must exist; (2) these technologies must be deployed; and (3) the implementation of these technologies must have a privacy protecting default configuration. Legal rights in the United States should provide an incentive structure that encourages these developments.

But new legal rights and technological protections in the United States will not be sufficient to resolve the trans-Atlantic privacy conflicts on a long-term basis. Any legal rights created in the United States will be defined in terms of the U.S. governance system—including the American delineations among state, citizen, and market power. As a result, such rights will always have a degree of variance with foreign laws that are set within their own governance systems. For global e-commerce, even small differences can have dramatic consequences.[175] When differences are entrenched in national values for the governance of a society, only international law will be able to resolve the structural conflicts. Treaties are the inevitable legal instruments that enable nation-state policies to develop in harmony.

In conjunction with the establishment of a legal baseline in the United States, the United States should promote the negotiation of a "General Agreement on Information Privacy" (GAIP) within the World Trade Organization framework.[176] This treaty organization's mission covers e-commerce and can be used to facilitate the protection of citizens within the transborder data flows. Whether or not desired by various interest groups and countries, the WTO will be unable to avoid confronting international privacy issues as a result of the biennial ministerial conferences and the inevitable trade-in-services agenda. Many of

175. *See, e.g.*, REIDENBERG & SCHWARTZ, *supra* note 87, at 143–44 (discussing the distorting effects for online services of small divergences in national data protection law within Europe).

176. *See* Reidenberg, *supra* note 3, 1359–62 (advocating an international treaty on data privacy in the WTO framework instead of an international directorate).

the core differences among nations on the implementation of privacy principles touch upon fundamental governance and sovereignty questions.[177] These types of problems will only be resolved at an international treaty level like the WTO.

At this level, the WTO can define core standards for data protection. The WTO parties had a first experience with this standards-based approach to international trade law when intellectual property was added to the multilateral trade accord as a result of the Uruguay Round of trade negotiations.[178] The intellectual property agreement sets out the substantive standards for the protection of intellectual property each signatory must incorporate in its domestic law.[179] Once implemented, each signatory must abide by strict trade rules that recognize the protections afforded by the other signatories.[180] Similarly, the WTO could strive to establish a set of basic data protection standards—the GAIP—and incorporate them into the multilateral trade agreement. The incorporation of GAIP into the WTO and national law would then provide for mutual recognition of signatories' data privacy rules. This approach would have a higher likelihood of successfully facilitating e-commerce than any uniquely national or bilateral approach.

V. CONCLUSION

E-commerce poses tremendous challenges to the fair treatment of personal information in the United States, in Europe, and around the world. At present, the trans-Atlantic relationship for privacy is on a collision course. For all the problems found in U.S. data privacy, Europe cannot lay claim to the only possible system of protection for personal information, and the export restrictions found in European law will necessitate the ban of transborder data flows for a variety of e-commerce activities. The attempt to create an ad hoc "safe harbor" for transatlantic data flows, while laudable, falls far short of its goal. The legality of such an approach is dubious, the political commitment faces obstacles, and the commercial environment will be inhospitable for those American companies who might offer better protection to foreign-origin data than to

177. *Id.*

178. *See generally* Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations: Agreement Establishing the World Trade Organization (1994) (including the TRIPs annex on intellectual property.)

179. *Id.* at 358–59.

180. *Id.* at 359–60.

American-origin data. A new international data privacy treaty will be essential for the long-term, robust growth of e-commerce.