# RESTORING AMERICANS' PRIVACY IN ELECTRONIC COMMERCE

*By Joel R. Reidenberg* †

## ABSTRACT

In the United States today, substance abusers have greater privacy than web users and privacy has become the critical issue for the development of electronic commerce. Yet, the U.S. government's privacy policy relies on industry self-regulation rather than legal rights. This article argues that the theory of self-regulation has normative flaws and that public experience shows the failure of industry to implement fair information practices. Together the flawed theory and data scandals demonstrate the sophistry of U.S. policy. The article then examines the comprehensive legal rights approach to data protection that has been adopted by governments around the world, most notably in the European Union, but finds that difficulties implementing these laws for online services pose important challenges for the effective protection of citizens' privacy. The lessons show that safeguarding citizens' rights requires a combination of law and technology and that a legal incentive structure is necessary to stimulate the rapid development and implementation of privacy-protecting technologies. The article concludes with a recommendation for a framework privacy law in the United States modeled on the O.E.C.D. guidelines that includes a safe harbor provision for policies and technologies and that creates a U.S. Information Privacy Commission to assure the balance between citizens' privacy, industry needs, and global competitiveness.

Privacy is a critical issue for the growth of electronic commerce. During the last few years, an overwhelming majority of Americans report that they have lost control of their personal information and that current laws

---



† Professor of Law and Director of Graduate Program Academic Affairs, Fordham University School of Law. An earlier draft of this paper was presented at the University of California, Berkeley Symposium *The Legal and Policy Framework for Global Electronic Commerce: A Progress Report* held March 4-6, 1999. I am very grateful for the thoughtful comments of Symposium participants and of the editors of the *Berkeley Technology Law Journal.*

are not strong enough to protect their privacy.[1] In 1998, *Business Week* found that consumer worries about protecting privacy on the Internet ranked as "the top reason people are staying off the Web above cost, ease of use and annoying marketing messages."[2] The fair treatment of personal information and citizen confidence are each necessary conditions for electronic commerce over the next decade. Yet, sadly, at the political birth of the electronic commerce movement in 1997, the White House's report, *A Framework for Global Electronic Commerce*,[3] more commonly referred to as the Magaziner Report, missed a key opportunity to assure the protection of citizens' privacy on the Internet.

For years, the United States has relied on narrow, ad hoc legal rights enacted in response to particular scandals involving abusive information practices.[4] The approach has led to incoherence and significant gaps in the protection of citizens' privacy.[5] For example, substance abusers have stronger privacy rights than web users in the United States.[6] Yet, rather than revise American privacy protection, the Magaziner Report adopted a position enshrining the status quo.

This paper will first examine the philosophy and sophistry behind the U.S. policy of industry self-regulation. Next, the paper examines the com-

---

1. Privacy Exchange.org, *1998 Privacy Concerns & Consumer Choice Survey, Executive Summary*, at 1 (last modified Dec. 15, 1998) <http://www.privacyexchange.org/iss/surveys/1298execsum.html> (reporting that 82% of those surveyed feel that consumers have lost all control over how companies collect and use their personal information); Am. Ass'n. of Retired Persons, *AARP Members' Concerns about Information Privacy*, Dec. 1998 (reporting that 78% of those polled found existing statutory protections inadequate to protect privacy).

2. *BW/Harris Poll: Online Insecurity*, BUS. WK., Mar. 16, 1998, at 102 <http://www.businessweek.com/1998/11/b3569107.htm>.

3. WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), *available at* <http://www.iitf.nist.gov/eleccomm/ecomm.htm> [hereinafter FRAMEWORK].

4. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 10 (1996).

5. *See generally* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997); SCHWARTZ & REIDENBERG, DATA PRIVACY LAW, *supra* note 4.

6. Federal law carefully protects the personal information of individuals who undergo treatment for alcohol or drug abuse in programs receiving federal funds or subject to federal regulation. *See* 42 U.S.C. §§ 290dd-1, 290dd-2 (1994); SCHWARTZ & REIDENBERG, DATA PRIVACY LAW, *supra* note 4, at 177-78. At the same time, only limited protection is available for Internet users. Statutory protection applies to telecommunications transaction information when collected by telecommunications service providers. *See* 47 U.S.C. § 222. However, if the data is collected by web sites, instead of service providers, then the statutory protection does not apply.

prehensive legal rights approach to data protection that has been adopted by governments elsewhere around the world, in a movement led by the European Union. While conceptually the cross-sectoral approach is better suited to the treatment of personal information in electronic commerce, the foreign experience illustrates a number of challenges for effective protection of citizens. The concluding section argues for a more desirable policy that combines legal and technological means in order to safeguard the privacy of citizens on the Internet.

## I. THE PHILOSOPHY AND SOPHISTRY OF U.S. PRIVACY POLICY

Broad, international consensus exists on the basic standards of fair information practice and the protection of citizen privacy in a democratic society.[7] As recently as June 1998, the Clinton Administration even said that the "O.E.C.D. Guidelines have served as the basis for virtually all privacy legislation and codes of conduct that have been developed over the years."[8] Beginning with the U.S. Department of Health and Education's elaboration of the first computer privacy policy in 1973[9] and the United States' approval of the Organization for Economic Co-Operation and Development's privacy guidelines in 1980, the United States has recognized benchmark norms for fair information practice. These norms include specification of the purpose for data collection, the consent of individuals to process personal information, the transparency of data processing, such as notice to individuals and access to their personal information, special

7. *See* Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, Jan. 28, 1981, EUR. T.S. No. 108, *reprinted in* 20 I.L.M. 377 (1981), *available at* <http://www.coe.fr/eng/legaltxt/108e.htm> [hereinafter *European Convention*]; 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, 1995 O.J. (L281) 31 (Nov. 23, 1995), *available at* <http://europa.eu.int/eur-lex/en/lif/dat/en_395L0046.html> [hereinafter *European Directive*]; O.E.C.D., RECOMMENDATIONS OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, O.E.C.D. DOC. C58 (final) (Oct. 1, 1980), *reprinted in* 20 I.L.M. 422 (1981), *available at* <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.htm> [hereinafter *OECD Guidelines*].

8. U.S. DEPT. OF COMMERCE, PRIVACY AND ELECTRONIC COMMERCE (June 1998) <http://www.doc.gov/ecommerce/privacy.htm>.

9. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens* (1973), *reprinted in* U.S. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, 15 n.7 (1977).

treatment of particularly sensitive information, such as medical data, and the existence of enforcement remedies and mechanisms.

The United States, however, has rejected all attempts to legislate any full set of standards.[10] Rather, Congress and state legislatures have enacted isolated and narrow statutes such as the Fair Credit Reporting Act[11] and the Video Privacy Protection Act,[12] after the discovery of particularly scandalous practices. This type of statutory protection only covers the particular activities committed by specific actors such as a consumer credit reporting agency or a video rental service provider. This reactive policy for 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. The theory holds that the marketplace will protect privacy because the fair treatment of personal information is valuable to consumers; in other words, industry will seek to protect personal information in order to gain consumer confidence and maximize profits.[13]

For more than twenty years, however, government agency task forces and reports regularly illustrated the lack of fair information practices in American society, but nevertheless resorted to the mantra that business should be given more time to self-regulate.[14] With the Internet revolution,

---

10. *See* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199 (1993).

11. 15 U.S.C. § 1681 (Supp. 3).

12. 18 U.S.C. § 2710-2711 (1994).

13. *See, e.g.*, U.S. DEPT. OF COMMERCE, NAT'L TELECOMM. AND INFO. ADM., PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, Ch. I.A (June 1997) <http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm>.

14. *See, e.g.*, U.S. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977); FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998) <http://www.ftc.gov/reports/privacy3/toc.htm>; INFORMATION POLICY COMMITTEE, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (Apr. 1997) <http://www.iitf.nist.gov/ipc/privacy.htm>; FEDERAL TRADE COMMISSION, STAFF REPORT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE (Dec. 1996) <http://www.ftc.gov/reports/privacy/privacy1.htm>; NAT'L TELECOMM. AND INFO. ADM., U.S. DEPT. OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (Oct. 1995) <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>; U.S. ADVISORY COUNCIL, NATIONAL INFORMATION INFRASTRUCTURE, COMMON GROUND: FUNDAMENTAL PRINCIPLES FOR THE NATIONAL INFORMATION INFRASTRUCTURE (Mar. 1995) ; U.S. INFORMATION INFRASTRUCTURE TASK FORCE WORKING

the Clinton Administration had a chance to conceive a new vision of American privacy. Unfortunately for American citizens, the Magaziner Report sought to preserve the status quo:

> The Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy.[15]

In effect, the Magaziner Report catered to the industry of personal data rather than enshrining citizen participation in decisions about their personal data. Indeed, the marketplace of personal information is big business in the United States. By 1998, the gross annual revenue of companies selling personal information and profiles, largely without the knowledge or consent of the individuals concerned, was reportedly $1.5 billion.[16]

Despite the claims of industry partisans, there are critical normative flaws in the theory of self-regulation for information practices. Self-regulation assumes that all privacy values can and should be resolved by a marketplace. Yet privacy interests are central to democratic governance[17] and privacy has been hailed as a necessary condition for participatory governance.[18] In contrast, totalitarian governments prefer the surveillance state.[19] Indeed, a democratic government typically does not sell basic political rights. But even if one rejects this position, a marketplace can only function efficiently if there is transparency; citizens must be able to identify the collectors and users of their personal information. However, for personal information, the natural tendency of the marketplace is to obscure its treatment.

This is a classic case of market failure. Without disclosure by corporations, citizens cannot ascertain how their personal information is acquired and used. In the private sector, the economics are wrong for transpar-

---

GROUP ON PRIVACY, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (Oct. 1995) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>.

15. FRAMEWORK, *supra* note 3, at 14 (Issue 5).

16. *See In re Trans Union*, FTC Docket No. 9255, at 53 (July 31, 1998) <http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf>.

17. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 23-26 (1967).

18. *See* Paul Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 732 (1987).

19. *See* WESTIN, *supra* note 17, at 23.

ency.[20] Companies make significant profits from the secret collection and sale of personal information; the $1.5 billion market in personal information is largely hidden from public view. Few individuals have ever heard of companies such as Acxiom or First Data. Yet, these companies have data warehouses with the most intimate details of the lives of millions of Americans. For example, Acxiom even sells information such as ethnic and religious affiliations, the type of car a person drives, and whether a person buys specialty clothing like particular types of underwear.[21] Without transparency, an information trafficking industry has emerged in the United States with no accountability and minimal risk of harm to corporate financial interests from abuses of personal information. Not surprisingly, an analysis of industry codes of privacy practice reveals policies that fail to address the most basic principles of citizens' rights to personal information.[22]

In effect, the American experience during the last two decades shows that the theory of self-regulation is pure sophistry. Time and again, the U.S. government has acknowledged that self-regulation remains hypothetical in corporate America. The Department of Commerce held a long awaited *Public Meeting on Internet Privacy* in June 1998, initially designed to give industry a chance to show its self-regulatory successes.[23] Unfortunately, industry had very little to show in terms of concrete implementation of privacy practices and the Secretary of Commerce conceded that the business community was failing to demonstrate effective self-regulation.[24] The Chairman of the Federal Trade Commission, in testimony to Congress during the summer of 1998, stated that "despite the Commission's considerable efforts to encourage and facilitate an effective

---

20. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1248 (1998) (observing that transaction costs are ignored in the market-based solutions); Paul Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997).

21. *See Acxiom Catalog*, at 9 (ethnic data), 11 (specialty apparel data), 12-13 (car data) (1999) <http://www.acxiom.com/infobase/catalog/catalog99.pdf> (PDF file).

22. *See* Joel R. Reidenberg & Paul M. Schwartz, *Legal Perspectives on Privacy*, *in* INFORMATION PRIVACY: LOOKING FORWARD, LOOKING BACK (Mary Culnan & Robert Bies eds., forthcoming 1999) (noting particular failure of industry codes to encompass significant amounts of personal information and the failure to include remedies for victims of information abuse).

23. *See* U.S. DEPT. OF COMMERCE, *Agenda for Public Meeting on Internet Privacy* (June 23-24, 1998) <http://www.ntia.doc.gov/ntiahome/privacy/confinfo/agenda.htm>.

24. *See* Commerce Secretary William H. Daley, Remarks to Privacy Summit (June 23, 1998) (transcript available at <http://www.doc.gov/opa/Speeches/980623.html>).

self-regulatory system, we have not yet seen one emerge."[25] Several months later, the first government review of the position paper *A Framework for Global Electronic Commerce* wistfully admits that industry has only tentatively responded to privacy concerns even in the face of heavy government pressure.[26]

It is worthy to note, however, that industry has improved its privacy talk over the last few years. Trade associations are now addressing the issues of data privacy (and lobbying Congress against regulation). The Secretary of Commerce has also tried to highlight self-regulatory initiatives such as TRUSTe and BBBOnLine as evidence of progress.[27]

But, ironically, these examples themselves demonstrate the structural defects in self-regulatory theory. TRUSTe, for example, is a program through which websites agree to disclose their privacy policies and license the right to use a special logo designating the site as one that protects privacy.[28] TRUSTe may audit licensees to verify compliance with the stated privacy policy. However, the program has had a few major problems. Although about 450 companies are licensed to use the logo to date, this number is trivial compared to the number of website operators in the United States. In fact, one of the companies, GeoCities, holds the distinction of being the first company prosecuted by the Federal Trade Commission for information trafficking,[29] and fifty percent of the TRUSTe sponsors do not bother to subscribe to the program and license the logo.[30] TRUSTe even features a link on its web page to a look-up service site that

---

25. *Electronic Commerce: Privacy in Cyberspace, Hearings on H.R. 2368 Before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Comm. on Commerce*, 105 Cong., 2nd Sess., July 21, 1998 (testimony of Robert Pitofsky, Chairman of the FTC), *available at* <http://www.ftc.gov/os/1998/9807/privac98.htm#N_3_>.

26. U.S. GOV'T WORKING GROUP ON ELEC. COMMERCE, FIRST ANNUAL REPORT 16 (Nov. 1998), *available at* <http://www.doc.gov/ecommerce/E-comm.pdf>.

27. *See* Commerce Secretary William H. Daley, Remarks at Press Conference on E-Commerce (Feb. 5, 1999) (transcript available at <http://www.doc.gov/opa/Speeches/ecommerceremarks.html>).

28. *See* TRUSTe, *TRUSTe Program Principles* (visited Mar.30, 1999) <http://www.truste.org/webpublishers/pub_principles.html>.

29. *See In re GeoCities Decision and Order*, F.T.C. Docket No. C-3850 (visited Mar.29, 1999) <http://www.ftc.gov/os/1999/9902/9823015d&o.htm>.

30. As of March 2, 1999, TRUSTe had 51 sponsors; only 26 were registered as licensees of the TRUSTe logo to show a commitment to privacy. *Compare* TRUSTe, *TRUSTe Sponsors* (visited Mar. 30, 1999) <http://www.truste.org/about/about_sponsors.html>, *with* TRUSTe, *Look Up A Company* (visited Mar.30, 1999) <http://www.truste.org/users/users_lookup.html>.

fails to disclose its privacy policy and is owned by a company that is not even listed as a TRUSTe licensee.[31]

A similar pattern exists at BBBOnLine, a project of the Better Business Bureau proposed more than a year ago in response to U.S. government pressure on industry to demonstrate that self-regulation might work.[32] BBBOnLine hopes to provide an enforcement mechanism for privacy disputes online. However, for the moment, the BBBOnLine mechanism remains hypothetical. While the program officially launched on March 17, 1999,[33] BBBOnLine ignores the issue that consent might not be an appropriate basis for the processing of some personal information, such as health data, only requires that websites disclose particular practices, fails to require that remedies be afforded to victims of information abuse, and fails to require that individuals be granted complete access to their personal information.[34] In addition, BBBOnLine uses a nebulous and undefined term, "individually identifiable information," to circumscribe the scope of its participants' obligations. It also remains to be seen whether the online industry will participate on significant scale.

Another important privacy initiative likewise remains unavailable even after three years of development and government encouragement. Internet labeling and filtering technology based on the world wide web's protocol, Platform for Internet Content Selection ("PICS,") has been under development for a privacy application, the Platform for Privacy Preferences

---

31. TRUSTe requires that "web sites ... must disclose their personal information collection and privacy practices." TRUSTe, *The TRUSTe Program: How it Protects Your Privacy* (visited Mar. 30, 1999) <http://www.truste.org/users/users_how.html>. However, from the main TRUSTe member directory web page, TRUSTe, *Member Directory* (visited Mar. 30, 1999) <http://www.truste.com>, there is a link to <http://www.worldpages.com/whitepages>. This latter site allows a user to search for the address and phone number of anyone in the United States. The site does not display a TRUSTe logo, nor does it disclose any privacy policy. There is a link in fine print at the bottom of the web page *About Worldpages* to another web page: <http://www.worldpages.com/docs/about.whtml> (visited Mar. 30, 1999). This last web page similarly says nothing about privacy, but does identify the owner of the page: Web YP, Inc. Web YP, Inc. is not listed as a licensee of TRUSTe, though a company identified as "World Pages, Inc." is listed.

32. *See* BBBOnLine, *Homepage* (visited Mar. 31, 1999) <http://www.bbbonline.com>.

33. *See* Robert O'Harrow, *Better Business Bureaus Offer Online Privacy Seal*, WASH. POST, Mar. 17, 1999, at E1.

34. *See* BBBOnLine, *Eligibility Criteria for BBBOnLine Privacy Seal* (visited Mar. 31, 1999) <http://www.bbbonline.com/businesses/privacy/eligibility.html>.

("P3P"), since 1996.[35] The World Wide Web Consortium ("W3C")[36], an influential standards setting body for the Internet, has led the development effort for P3P technology. Yet after three years, W3C has still not obtained sufficient industry agreement to conclude the development phase, let alone find companies willing to implement the technology. In addition, P3P faces a patent licensing problem that jeopardizes its ultimate adoption by industry.[37]

The cornerstone of these self-regulatory efforts and U.S. policy seems to be the concept that notice and consent will solve the privacy issues. In describing the notice principle, the Magaziner Report articulates that "[d]ata-gatherers should inform consumers what information they are collecting, and how they intend to use such data."[38] The report describes the consent standard by asserting that "[d]ata gatherers should provide consumers with a meaningful way to limit use and re-use of personal information."[39] The Magaziner Report even argues that "principles of fair information practice [] rest on the fundamental precepts of awareness and choice."[40] This position is also emphasized clearly in the U.S. Department of Commerce's *Elements of Effective Self-Regulation.*[41] Yet, these pronouncements seriously misconstrue basic fair information practices principles. These basic principles include key standards, such as purpose limitations, data minimization, and duration of storage that are not satisfied merely through notice and consent; notice and consent are not enough. The United States has even recognized this broader range of issues when it endorsed the O.E.C.D. Guidelines.[42] In the rare instance when a government agency, the Federal Communications Commission,

---

35. *See* FEDERAL TRADE COMMISSION, TRANSCRIPT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE, F.T.C. PROJECT P954807, at 79-90 (June 4, 1996) (statement of Paul Resnick, AT&T Research) (transcript available at <http://www.ftc.gov/bcp/privacy/wkshp96/pw960604.pdf>).

36. *See* W3C, *About the World Wide Web Consortium* (visited Apr. 20, 1999) <http://www.w3.org/Consortium/>.

37. *See* Chris Oakes, *Patent May Threaten E-Privacy*, WIRED, Nov. 11, 1998, *available at* <http://www.wired.com/news/news/technology/story/16180.html>; Intermind, *About Intermind Communication's Patents* (visited Apr. 20, 1999) <http://www.intermind.com/materials/patent_desc.html>.

38. FRAMEWORK, *supra* note 3, at 12 (Issue 5).

39. *Id.*

40. *Id.*

41. *See* U.S. DEPT. OF COMMERCE, N.T.I.A., ELEMENTS OF EFFECTIVE SELF-REGULATION FOR PROTECTION OF PRIVACY (Jan. 1998) <http://www.ntia.doc.gov/reports Elements /privacydraft/198dftprin.htm>.

42. *See supra* note 8 and accompanying text; Gellman, *supra* note 10, at 200.

gave considered analysis to the effectiveness of consent as a legitimate basis for the sale of personal information to marketers, the FCC found opt-out to be a deficient basis for processing personal information under the Telecommunications Act of 1996 that mandated the protection of subscriber privacy.[43]

Thus, to rely principally on notice and consent ignores the other basic fair information practice principles and underlines how self-regulation has not worked. Indeed, for the online world, technological defaults routinely favor privacy invasions over the implementation of fair information practices for citizens. Recent examples, such as the incorporation by Intel of an embedded identifier on each of its Pentium III chips[44] and the "smart browsing" features of Netscape Communicator and Internet Explorer software that upload from the user's computer a hidden file containing the Internet addresses of sites visited by the user,[45] illustrate techniques that facilitate the surreptitious surveillance of citizens. These examples demonstrate that the full range of fair information practice principles are marginalized by self-regulation defined in terms of notice and consent. Smart browsing, for instance, confronts the basic principle of purpose limitations and storage duration as addresses, processed to make website connections, are stored beyond the duration of the connection and now uploaded to a remote site for profiling purposes.

These basic flaws in the theory and practice of the U.S. self-regulatory approach pose an increasingly troubling problem for companies developing electronic commerce. Electronic commerce is global, yet American privacy policy is at odds with the growing movement around the world to establish clear, comprehensive legal rights. Ironically, American companies' global electronic commerce activities face an heretical choice: either provide better protection for U.S. citizens in order to have a single set of practices for global operations (because foreign laws require fair information practices) or maintain a double standard, treating foreign citizens to better privacy than U.S. citizens. The Magaziner Report largely ignores

---

43. *See* FCC Second Report and Order and Further Notice of Proposed Rulemaking, FCC Docket No. 96-149, ¶ 91 (Feb. 19, 1998) <http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt>.

44. *See* Jeri Clausing, *After Intel Chip's Debut, Critics Step Up Attack*, N.Y. TIMES ON THE WEB (Feb. 19, 1999) <http://www.nytimes.com/library/tech/99/02/cyber/articles/19intel.html>.

45. *See* Netscape Corp., *What's Related FAQ* (visited Apr. 20, 1999) <http://home.netscape.com/escapes/related/faq.html#o6>.

this incongruity in boldly assuming that the rest of the world would simply accept the U.S. status quo with better educational efforts.[46]

The international consequence of this self-regulatory pretense is an embarrassment for the U.S. government. Without demonstrable privacy protection in the United States, Europe threatens to block the flow of personal information to the United States.[47] The U.S. Department of Commerce has sought to negotiate with the European Commission a "safe harbor" code that would assure privacy for international data transfers to the United States and avoid any European data export prohibitions.[48] The proposal met with resounding criticism and virtual ridicule for its lack of content.[49] Because the Department of Commerce cannot propose any meaningful privacy standards, such as implementation mechanisms or enforcement devices providing remedies to victims, without undermining support for self-regulation, it is unequipped to respond to such criticism. Yet, without meaningful privacy standards, the United States isolates itself from the rest of the world. The time has come to reevaluate and reverse the policy that enshrines electronic surveillance and information trafficking against citizens.

## II. THE CHALLENGE OF COMPREHENSIVE LEGAL STANDARDS

The recycling of unsuccessful and outdated privacy policies in the United States is in direct contrast to the data protection movement around

---

46. *See* FRAMEWORK, *supra* note 3, at 14 (Issue 5) ("The United States will continue policy discussions ... to increase understanding about the U.S. approach to privacy and to assure that the criteria [Europeans] use for evaluating adequacy are sufficiently flexible to accommodate our approach.").

47. *See European Directive*, *supra* note 7, at art. 25.

48. *See* U.S. Dept. of Commerce, *Draft International Safe Harbor Privacy Principles* (Nov. 4, 1998) <http://www.ita.doc.gov/ecom/menu.htm>.

49. *See* International Trade Administration, U.S. Dept. Of Commerce, *Public Comments filed on "Draft International Safe Harbor Privacy Principles"* <http://www.ita.doc.gov/ecom/com.htm>; Working Party of European Data Protection Supervisory Authorities, *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussion between the European Commission and the United States Government*, DG XV 5092/98/WP15 (Jan. 26, 1999) <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp15en.htm>; Working Party of European Data Protection Supervisory Authorities, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98/WP12 (July 24, 1998) <http://europa.ue.int/comm/dg15/en/media/dataprot/wpdocs/wp12en.htm>.

the world. Foreign countries, led by the fifteen states of the European Union (the "Member States"),[50] more typically follow an omnibus or comprehensive approach. Ironically, Europe learned its post-war lessons about information privacy from the movement in the United States during the 1960s and 1970s.[51] But, unlike the United States, as European countries faced the computer processing of large quantities of personal information in the 1970s and 1980s, they adopted comprehensive data protection statutes to enshrine a rights-based, rather than market-based, approach to privacy. Indeed, in 1981, the Council of Europe opened for signature and ratification a data privacy treaty that has as its object and purpose "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data."[52]

Under the European model, framework legislation guarantees a broad set of rights to assure the fair treatment of personal information and the protection of citizens. In general, the modern European data protection laws define each citizen's basic legal right to "information self-determination."[53] 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. Rather than accord pre-eminence to business inter-

50. These states are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

51. *See, e.g.*, COLIN BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989); Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest* 80 IOWA L. REV. 431 (1995).

52. *European Convention*, *supra* note 7, at art. 1.

53. This term "information self-determination" was coined by a 1983 German court decision prohibiting the intrusiveness of a national census. *See* Judgment of the First Senate [Bverfge, Karlsruhe], Dec. 15, 1983, *translated in* 5 HUM. RTS. L.J. 94 (1984).

ests, the European approach seeks to provide for a high level of protection for citizens.[54]

Although the comprehensive rights approach has conceptual appeal for electronic commerce, it poses normative challenges for the structure of electronic commerce ventures and the effective protection of citizens. Because the rights-based approach relies on omnibus legislation, it covers the electronic processing of personal information regardless of context.[55] These statutes apply the same standards of fair treatment for personal information across sectoral boundaries of collection and use. In theory, this cross-sectoral application of principle correlates well to an information society where industry boundaries blur and data use defies clear categorization.

However, with the proliferation of European data protection laws during the course of the last two decades, the national laws evolved[56] and different standards in various Member States threatened the flow of personal information within Europe. For example, the scope of application of data protection laws and transparency requirements varied across national laws, posing conflicts for pan-European data processing.[57] In response, the Member States of the European Union sought to harmonize data protection principles and launched a five-year negotiating process that ultimately resulted in the enactment of the European Directive on data protection.[58]

The European Directive confirmed the pre-existing comprehensive rights-based approach and contained both general and exacting rules aggregated from the laws of various European Union Member States.[59] Like the existing national laws, the European Directive's rules address the full set of internationally recognized principles. Each Member State must enact legislation implementing standards conforming to those defined by the

---

54. *See, e.g., European Directive, supra* note 7, at Recital 10 (explaining that the purpose of the Directive is to "seek to ensure a high level of protection in the Community").

55. *See id.*, at Recital 12, art. 3.

56. *See* Viktor Mayer-Schonberger, *Generational Development of Data Protection in Europe, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 220 (Philip E. Agre & Marc Rotenberg eds., 1998).

57. *See European Directive, supra* note 7, at Recital 7; JOEL R. REIDENBERG & PAUL M. SCHWARTZ, DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES (Eur. Comm. 1998), *available at* <http://europa.eu.int/comm/dg15/en/media/dataprot/studies/regul.pdf>.

58. *See European Directive, supra* note 7.

59. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995).

European Directive,[60] and each Member State must maintain an independent, national supervisory authority for oversight and enforcement of these privacy protections.[61] Significantly, the European Directive also mandates that Member State law require any person processing personal information to notify the supervisory authority and the supervisory authority must keep a public register of data processors.[62]

While the harmonization of European data protection around comprehensive standards seems conceptually better suited to electronic commerce, in practice, the complexity of data processing arrangements in an information society makes the application of general principles to particular contexts challenging. Indeed, the registration mechanisms designed to assure transparency of processing activities can become onerous and problematic. Within Europe, critics have argued that compliance with these registration obligations is lacking.[63] Elsewhere, required notification to a government agency of data collection might be seen as an overly intrusive government action. In the United States, for example, the European commitment to the registration of data processing activities with a government agency would clash with Fourth Amendment values against government intrusion into the activities of citizens.

Furthermore, the application of the European Directive does not remove all divergences and ambiguities in the European national laws.[64] Small divergences and ambiguity will inevitably exist where the principles must be interpreted by different supervisory organizations in each of the Member States. These remaining divergences in standards can pose significant obstacles for the complex information processing arrangements typical in electronic commerce. For example, the European Directive requires that privacy rights attach to information about any "identifiable per-

60. This 'transposition' of the European Directive's standards into national law was to have occurred by October 1998. *See European Directive*, *supra* note 7, at art. 32. However, as is not uncommon in the European system, few Member States have complied with the deadline.

61. *See European Directive*, *supra* note 7, at art. 28.

62. *See id.* at art. 18-19.

63. *See 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., Eur. Comm: 1998).

64. *See* REIDENBERG & SCHWARTZ, DATA PROTECTION LAW, *supra* note 57; PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 188-96 (1998).

son."[65] Yet, the scope of this definition is not the same across the Member States; what some Member States consider "identifiable" others do not.[66] Similarly, the disclosures that must be made to individuals prior to data collection vary within Europe.[67] These differences distort the ability and desirability of performing processing operations in various Member States since 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 under the European model. The European Directive creates a working party of the Member States' data protection commissioners.[68] The Working Party offers a formal channel for data protection officials to consult each other and to reach consensus on critical interpretive questions. But, policy guidelines from the Working Party will not be sufficient to assure privacy in electronic commerce. Guidelines will not be meaningful in a dynamic network environment without a technical infrastructure that also promotes data protection. This has been recognized internationally by data privacy commissioners: "it is mandatory to develop design principles for information and communications technology ... which will enable the individual user to control ... his personal data."[69] Interestingly, the European model includes a provision for consensus on industry codes of conduct that might prove quite useful to facilitate the implementation of privacy compatible technologies.[70] The European Directive, building on Dutch law, provides for approval of codes of conduct as conforming to the privacy standards. This provision can be used to certify technical codes and configurations to assure privacy.[71] The use of such technical measures may also be designed to avoid problems found in standards divergence, such as the differences in notice requirements.[72]

---

65. *European Directive*, *supra* note 7, at art. 2(a).

66. *See* REIDENBERG & SCHWARTZ, DATA PROTECTION LAW, *supra* note 57, at 124-26.

67. *See id.* at 133-34.

68. *See European Directive*, *supra* note 7, at art. 29.

69. International Working Group on Data Protection and Telecommunications, *Data Protection and Privacy on the Internet: Report and Guidance* (Berlin, Nov. 18, 1996) <http://www.datenschutz-berlin.de/diskus/13_15.htm>.

70. *See European Directive*, *supra* note 7, at art. 27.

71. *See* REIDENBERG & SCHWARTZ, DATA PROTECTION LAW, *supra* note 57, at 147.

72. *See id.* at 153-54; Working Party of European Data Protection Supervisory Authorities, *Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, DG XV D/5032/98/WP11 (June 16, 1998) <http://europa.eu.int/

For global information networks and electronic commerce, the comprehensive approach also inevitably invokes 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 assure that personal information of European origin will be treated with European standards. The choice of law clause in the European Directive assures that the standards of the local state applies to activities within its jurisdiction and the transborder data flow provision prohibits the transfer of personal information to countries that do not have "adequate" privacy protection.[73] Some commentators have predicted that any European action will spark a trade war that Europe might lose before the new World Trade Organization.[74] While, in theory, such a situation is possible, it is equally remote.[75]

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.[76] This movement can be attributed partly to the pressure from Europe arising from scrutiny of the adequacy of foreign privacy rights, but is also partly due to the conceptual appeal of a comprehensive set of data

---

comm/dg15/en/media/dataprot/wpdocs/wp11en.htm>; Joel R. Reidenberg, *International Data Flows and Methods to Strengthen International Co-operation* (paper presented at the 20th International Conference of Data Protection Authorities, Santiago de Compostela, Spain) (Sept. 17, 1998) <http://home.sprynet.com/~reidenberg/idt.htm>.

73. *See European Directive*, *supra* note 7, at art. 4 (choice of law) and art. 25 (export prohibition).

74. *See* SWIRE & LITAN, *supra* note 64, at 188-96.

75. *See* Joel R. Reidenberg, *The Movement toward Obligatory Standards for Fair Information Practices in the United States, in* VISIONS FOR PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE (Colin Bennet & Rebecca Grant eds., 1999).

76. *See, e.g.*, 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); Council of Europe, Chart of Signatories and Ratifications (visited Apr. 20, 1999) <http://www.coe.fr/tablconv/108t.htm> (listing countries that have ratified the treaty on data privacy); Industry Canada, *Task Force on Electronic Commerce: The International Evolution of Data Protection* (Oct. 1, 1998) <http://e-com.ic.gc.ca/english/fastfacts/43d10.htm> (justifying the Canadian proposal for a comprehensive privacy law by reference to the European initiative); Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data (Privacy) Ordinance, Ch. 486 (visited Apr. 20, 1999) <http://www.pco.org.hk/ord/section_00.html> (displaying Hong Kong statute that follows the European comprehensive model).

protection standards. In effect, Europe has displaced the United States in setting the global privacy agenda with the enactment of the data privacy directive.

But, as illustrated by the European experience, the resolution of these difficulties cannot derive from law reform alone. In short, the comprehensive standards approach has two serious problems. First, general principles, while needed, leave significant margin for implementation and interpretation, especially in countries with very different legal cultures. For electronic commerce, any ostensibly small divergences in implementation or interpretation can generate significant distortions affecting the coverage for personal information and the incentives for protection by companies.[77] Second, the process to enact data protection law in Europe shows that adoption of legal rights is exceedingly slow. The existing European data protection directive took five years and transposition into national law was scheduled for three additional years.[78] In Internet time, these delays are generational.

## III. SAFEGUARDING CITIZENS' RIGHTS WITH A COMBINATION OF LAW AND TECHNOLOGY

The lessons from the American experience with self-regulation show that government cannot abdicate responsibility for the protection of citizens' privacy to a marketplace skewed in favor of sale of personal information. At the same time, the lessons from the European experience involving detailed comprehensive statutes illustrate that effective privacy does not end with a legislative enactment. The guarantee of privacy for citizens requires a combination of law and technology that affords mechanisms to assure the fair treatment of personal information.

In a democratic state, privacy is and remains a basic right of citizens.[79] In contrast to many other aspects of privacy, informational privacy is unique in that citizens cannot determine how their personal information is being used without access to internal activities of those processing the data. To paraphrase Justice Stewart, "I do not know it when I cannot see

---

77. *See* REIDENBERG & SCHWARTZ, DATA PROTECTION LAW, *supra* note 57, at 142-46.

78. *See European Directive*, *supra* note 7, at art. 32.

79. *See* Jeb Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989); *OECD Guidelines*, *supra* note 7, at Preamble ("Member countries have a common interest in protecting privacy and individual liberties."); Schwartz *supra* note 18; Simitis, *supra* note 18; WESTIN, *supra* note 17.

it."[80] As a consequence, the citizen confidence in the treatment of personal information that is so necessary for robust electronic commerce will not develop without a clear underlying set of rights.

To restore privacy for American citizens, the United States needs a framework that provides consistent fair information practices across different types of uses of personal information and different forms of processing arrangements. The United States government, however, need not try to reinvent fair information practice principles. The O.E.C.D. guidelines offer a full set of standards already recognized by the United States.[81] The content of these guidelines provides a clear basis and level playing field for citizen privacy, and the guidelines themselves have been praised as sensitive to business concerns.[82] These principles should be adopted in law as the American framework for information privacy.

Nevertheless, as both the American and European experiences show, technological capabilities and configurations hold the balance between effective fair treatment of personal information and defective privacy. Technical choices embed a set of policy rules for information flows in data processing systems. This "code"[83] or "lex informatica"[84] contained in the technical infrastructure has a direct rule-making effect on privacy. For ex-

---

80. *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (describing attempts to categorize pornographic materials as "I know it when I see it.").

81. *See O.E.C.D. Guidelines*, *supra* note 7; U.S. DEPT. OF COMMERCE, PRIVACY AND ELECTRONIC COMMERCE (June 1998) <http://www.doc.gov/ecommerce/privacy.htm> (recognizing the OECD Principles as the standard); U.S. Dept. of Comm., Nat'l Telecomm. and Info. Adm., *The Global Information Infrastructure: Agenda for Cooperation*, 60 Fed. Reg. 10359, 10367 (Feb. 24, 1995) (recognizing that the US accepts the OECD Principles).

82. After the O.E.C.D. adopted the guidelines, major U.S. companies subscribed to the principles. *See* GENERAL ACCOUNTING OFFICE, PRIVACY POLICY ACTIVITIES OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION AGENCY (Aug. 31, 1984) *cited in* Gellman, *supra* note 10, at 227 n.60; H.P. Gassman, *Vers un cadre juridique internationale pour l'informatique et autres nouvelles techniques de l'information*, ANNUAIRE FRANCAIS DE DROIT INTERNATIONAL 747, 750 (1985) (according to the author, who was a staff official at the O.E.C.D., 180 U.S. companies had subscribed to the O.E.C.D. guidelines).

83. *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L. J. 869, 898 (1996).

84. *See* Joel R. Reidenberg, *Governing Networks and Rule Making in Cyberspace*, 45 EMORY L. J. 911, 917-19, 929 (1996); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998) [hereinafter *Lex Informatica*].

ample, the protocol P3P[85] is designed to empower web users by giving them information about website privacy policies and affording web users choices in the provision of personal information. However, P3P can only be effective if fairly written and appropriately implemented. The technical way in which the P3P protocol allows the expression of privacy policies and the choices given to web users are value-based decisions.[86] Furthermore, the manner in which P3P is incorporated in browsers, including the default settings and the fashion by which websites actually describe their practices, are critical for fair treatment of personal information. The development of "cookies" and their ability to track users across the Internet is another example of policy rules embedded in technical standards.[87] The initial default settings built into browsers encouraged the secret transfer of user's information, and only when faced with scandal did the software developers increase users' control over the disclosure of information.[88] These cases show that the technology can "go either way." The availability of privacy-protective technologies and privacy-enhancing default settings must exist. Yet, industry has demonstrated its lethargy in developing and implementing these technologies. Already, P3P has been in the development stage for three years and wide-spread use of the standard is, at best, a long time away.

Government must, therefore, act in a fashion that assures technological development in a direction favoring privacy protections rather than privacy intrusions. During the debate over self-regulation, U.S. industry took privacy more seriously only when government threats of regulation were perceived as credible. For example, the threats and cajoling from the Federal Trade Commission was a key impetus for the development of the BBBOnLine, Online Privacy Alliance, and TRUSTe programs. But, despite deadline extensions for action by the Federal Trade Commission, none of these programs has yet to demonstrate accountability by their cor-

---

85. P3P is a protocol to enable disclosure and negotiation of the terms of consumer privacy between a web user and a web site collecting personal information. *See* W3C, *Platform for Privacy Preferences P3P Project* (visited Mar. 31, 1999) <http://www.w3.org/P3P>.

86. *See* Joel R. Reidenberg, *The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters for Data Protection*, LEX ELECTRONICA (Fall 1997) <http://www.lex-electronica.org/reidenbe.html>.

87. *See* Mark Slayton, *An Introduction to Cookies*, HOT WIRED, Nov. 7, 1996 <http://www.hotwired.com/webmonkey/webmonkey/geektalk/96/45/index3a.html>.

88. *See* James Glave, *Next Netscape Will Chew Cookies on Command*, WIRED NEWS, Feb. 22, 1997, *available at* <http://www.wired.com/news/news/technology/story/2196.html>.

porate members for violations of privacy to individuals.[89] Indeed, to the contrary, industry created policies tend toward privacy myopia in the development of new products. Intel, for example, seemed genuinely surprised by the outrage expressed against its planned use of an unique identifier on its Pentium III chips.[90]

With the enactment of a basic set of rights, the incentive structure for industry would shift to the development of effective protection for citizen privacy rather than the elaboration of vague policies to forestall corporate accountability. The existence of basic legal rights will force industry to deploy fair information practices that are well-balanced rather than skewed against citizens. To stimulate the quick development of privacy protecting system designs, these legal rights should allocate liability to companies that fail to develop and deploy privacy-enhancing technology.[91] In doing this, legal standards will create new markets and opportunities for the development of privacy protecting products.

In any case, the promotion of privacy-friendly technologies and the implementation of fair information practices in particular contexts and especially in the electronic commerce context require constant vigilance. While counterintuitive for many in the United States, a U.S. Information Privacy Commission is urgently needed. Privacy policy requires a forum with a clear mandate for independent judgment to build consensus on solutions in particular contexts and to arbitrate disputes among stakeholders. In addition, U.S. business interests need an advocate in the face of international data flows. For years, the United States has remained on the sidelines of the annual meeting of data protection commissioners from around the world because the United States has no privacy commission.

At present, no existing agency or department in the United States is well suited to the tripartite role of consensus builder, privacy arbitrator, and international advocate. The Department of Commerce, where international privacy policy is presently formed, may be politically expedient, but is inappropriate for the range of privacy issues in the Information Society. The Commerce Department does not, for example, have particular expertise or competence in health privacy issues or global flows of employee data and is notoriously captured by business interests at the expense of

89. None of the programs offers any damage remedy to individuals when the company adherents fail to fulfill their privacy commitments.

90. *See* Polly Sprenger, *Intel on Privacy: 'Whoops!'*, WIRED NEWS, Jan. 25, 1999 <http://www.wired.com/news/news/politics/story/17513.html>.

91. *See Lex Informatica*, *supra* note 86, at 584 (discussing the effect of liability and the structure of the Internet.).

citizens' concerns.[92] The State Department might be more appropriate for the foreign policy role, but has no expertise on the myriad of domestic privacy issues. Similarly, existing independent agencies such as the Federal Communications Commission would be poor choices for the centralization of privacy policy. The competence of these existing agencies is sectoral and each lacks expertise in cross-sectoral issues. The recent creation of a new position in the White House Office of Management and Budget is a good, but insufficient step.[93] Unfortunately, the new position is placed within the layers of the OMB bureaucracy and does not fulfill all the needed roles. Instead, the post has a coordinating role and does not have policy decision-making authority nor does the position have authority for the international negotiations with Europe.

If the United States hopes to protect effectively citizen privacy in electronic commerce, an independent privacy commission offers a number of attractive benefits both for citizens and businesses. The application of general privacy principles in the dynamic and complex online environment will inevitably require interpretation of the standards. Since a citizen's perspective may undervalue the interests of industry and society at large to information flows, while a corporate perspective will undervalue citizen's privacy, an independent privacy commission can offer critical guidance. In particular, such a commission can be accorded the authority to grant safe harbor protections for company practices.[94] Like a no-action letter from the Securities and Exchange Commission, a company seeking guidance and assurance that its policies are appropriate should be able to request approval from the privacy commission. Such an approval would mean that the practice conforms to the legal obligations for the fair treat-

92. For example, instead of publishing notice in the Federal Register for public comment on the draft international privacy principles, Undersecretary Aaron sent a letter, dated November 4, 1998, addressed "Dear Industry Representative" and posted it on a hidden web page several days later. *See* Letter from David Aaron, Undersecretary of Commerce to Industry Representatives (Nov. 4, 1998), *available at* <http://www.ita.doc.gov/ecom/aaron114.html>.

93. Declan McCullagh & James Glave, *Clinton Tabs Privacy Point Man*, WIRED NEWS, Mar. 3, 1999, *available at* <http://www.wired.com/news/news/politics/story/18249.html>.

94. *See* Joel R. Reidenberg, *Privacy in an Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 242 (1992) (proposing a legislative model with a safe harbor mechanism for industry).

ment of personal information. This safe harbor approach was recently endorsed by the Federal Trade Commission.[95]

In the context of electronic commerce, the safe harbor concept is especially powerful for guidance on technical infrastructure decisions. Technical protocols, default settings, and implementations can be treated the same way as company practices and policies for purposes of a safe harbor.[96] The existence of such a voluntary approval mechanism would give companies an important tool to avoid myopic, internal evaluations of the privacy ramifications, protect against data scandals, insulate the company from liability for privacy invasions, and satisfy foreign privacy regulators such as those in the European Union.

At the same time, the safe harbor process would afford citizens an opportunity for public comment on the conformity of practices to framework legal obligations and would not immunize practices outside the safe harbor nor immunize those safe harbor practices that change. Over time, safe harbor decisions would develop a body of public guidance that would increase transparency for all citizens. For citizens, the independent commission and a safe harbor procedure would also assure that the interpretation of fair information practices for electronic commerce continues as an ongoing process.

## IV. CONCLUSION

The time has come for the U.S. government to become serious about privacy and restore protection to citizens. The Magaziner Report clearly erred in charting a conventional approach for a most unconventional, new environment. Citizens participating in global electronic commerce need to be assured that their personal information will be treated fairly. Companies engaged in electronic commerce cannot be crippled in their use of personal information. Fundamental values are at stake and one-sided policies and solutions will undermine democratic society.

---

95. *See Electronic Commerce: Privacy in Cyberspace, Hearings on H.R. 2368* Before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Comm. on Commerce, 105th Cong., 2nd Sess., July 21, 1998 (testimony of Robert Pitofsky, Chairman of the FTC), *available at* <http://www.ftc.gov/os/1998/9807/privac98.htm#N_3_>.

96. *See, e.g.*, REIDENBERG & SCHWARTZ, DATA PROTECTION LAW, *supra* note 57, at 153-54.