The John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 1

Fall 2000

The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective, 19 J. Marshall J. Computer & Info. L. 1 (2000)

William S. Challis

Ann Cavoukian

ARTICLES

THE CASE FOR A U.S. PRIVACY COMMISSIONER: A CANADIAN COMMISSIONER'S PERSPECTIVE

by WILLIAM S. CHALLIS, LEGAL COUNSEL, &
DR. ANN CAVOUKIAN, COMMISSIONER
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

I. THE DIMENSIONS OF THE ISSUE

The debate over Internet privacy has reached a fever pitch and the temperature is still rising. The demands of social democratic government, the appetite of electronic commerce, and the ingenuity of the human mind have conspired to create information technologies at once useful and compliant, powerful and frightening. The exponential growth of the Internet[1] has generated vast collections of personal information and concomitant threats to privacy on a global scale: surveillance, profiling and identity theft, to name a few. Rapid technological advances in search engines, indexing, data warehousing and data mining have accelerated this trend.[2] These technologies offer unprecedented opportunities for enlightenment, prosperity and enhancement of personal well being. They can also become awesome tools of abuse. Stakeholders are strewn along all shades of the political spectrum, at all levels of the economic topography, and among all reaches of cyberspace.

The debate has focused on the efficacy of industry self-regulation

1. Nua Internet Survey, *How Many Online*, <http://www.nua.ie/survey/how_many_online/index.html> (accessed May 29, 2000) (noting that as of May 2000, it is estimated that over 300 million users are online globally, close to half of these in North America); *see also* DomainStats.com, *Latest Domain Stats*, <http://www.DomainStats.com> (last updated Sept. 5, 2000) (noting that at present, there are approximately 16 million domains registered worldwide); Censorware Project, *Size of the Web: A Dynamic Essay for a Dynamic Medium* <http://www.censorware.org/web_size/> (last updated Sept. 12, 2000) (noting that the volume of material available on the Internet is estimated to be more than doubling every year).

2. Federal Trade Commission, *Final Report of the FTC Advisory Committee on Online Access and Security* <http://www.ftc.gov/acoas/papers/finalreport.htm> (accessed Nov. 10, 2000).

versus state regulation: the present U.S. model[3] versus the model reflected in the European Union's Directive on the Protection of Personal Data (the European Directive)[4] and beginning to emerge in other nations' data protection laws.[5] Recent developments have given added impetus to state regulation: studies on the pervasiveness of online collection, sharing and sale of personal data; studies on the prevalence, consistency and adequacy of Web site privacy polices;[6] consumer surveys

3. *Privacy Act*, 5 U.S.C. §552 (1994); *Fair Credit Reporting Act*, 15 U.S.C. §§ 1681-1688t (1994); *Freedom of Information Act*, 5 U.S.C. § 552 (2000); *Family Educational Rights and Privacy Act*, 20 U.S.C. § 1232g (1994); *Right to Financial Privacy Act*, 12 U.S.C.S. § 3412 (2000); *Privacy Protection Act*, 42 U.S.C. §2000aa (2000); *Electronic Communications Privacy Act*, Pub. L. No. 99-508, 100 Stat. 1848-73 (1986); *Video Privacy Protection Act*, 18 U.S.C. § 2710 (1994); *Employee Polygraph Protection Act*, 29 U.S.C.S. §§ 2001 et seq. (2000); *Cable Communications Policy Act*, 47 U.S.C. §551(h) (2000); *Telephone Consumer Protection Act*, 47 USCS § 222 (2000); *Drivers' Privacy Protection Act*, Pub. L. No. 103-322; 108 Stat. 1796 (1994); *Financial Services Modernization Act*, Pub. L. No. 106-102, 113 Stat. 1338 (1999); *The Children's Online Privacy Protection*, 15 U.S.C. §§ 6501-6506 (1999) (governing the special case to which its title refers). Privacy protection on the Internet has largely been left to industry self-regulation, which has received strong encouragement and support from the Federal Trade Commission, the U.S. Department of Commerce and the White House. *Id.* The Federal Trade Commission may also assert jurisdiction over Internet Privacy issues under section 5(a) of the *Federal Trade Commission Act*, 15 U.S.C. § 45(a) where deceptive and unfair practices are involved. *Id.*

4. Directive 95/46/EC of the European Parliament and the Council of Oct. 24, 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 281/33) ¶ 24 (noting the Directive's focus on the protection of individuals with regard to the processing of personal data and on the free movement of such data) [hereinafter "Directive 95/46/EC"].

5. *See e.g.*, *Personal Information Protection and Electronic Documents Act*, S.C. ch. V (2000) (Can.) (assented to Apr. 13, 2000) (available at <http://www.privcom.gc.ca/english/02_06_01_01_e.htm>); The Australian Privacy Commission, *Australia's Privacy Amendment (Private Sector) Bill 2000*, <http://www.privacy.gov.au/private/index.html> (last modified Nov. 28, 2000); The Privacy Commissioner's Office, *Personal Data (Privacy) Ordinance*, Ch. 486, <http://www.pco.org.hk/ord/section_00.html> (accessed Nov. 27, 2000); Confoederatio Heletica, *Loi federale sur la protection des données* (19 Juin 1992) 235.1 <http://www.admin.ch/ch/f/rs/235_1/index.html> (accessed Nov. 27, 2000); *see infra* n. 137 (explaining that most members of the European Community have data protection laws governing the private sector, many of which have required amendment to bring them into compliance with the requirements of the European Directive); David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 John Marshall J. of Computer & Info. L. 1 (1999) (providing a comprehensive survey of data protection laws as of 1999).

6. Federal Trade Commission Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, 2-3, 7-24, Appendix A <http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf> (May 2000) (noting that recent studies commissioned by the Federal Trade Commission find that only 20% of the busiest commercial Web sites implement all four fair information practices (notice, consent, access, and security) and only 42% of the most popular sites did so, and only 8% of the busiest sites and only 42% of the most popular sites displayed any kind of privacy seal, and only 14% of all surveyed Web sites disclosed anything at all about their information practices).

showing widespread confusion and concern about online privacy protections;[7] demonstrated limitations of privacy policies and seal programs;[8] questions about the proper role of the U.S. Federal Trade Commission in overseeing U.S. consumer privacy policy;[9] and the European Union's reluctant acceptance of U.S. "safe harbor" policies.[10] These developments and others have spawned a proliferation of Internet privacy bills in the 106th Congress. No fewer than 14 bills affecting online privacy regulation are now before the House or Senate, some of general application, others limited to specific sectors or communications media.[11] Still other

7. Cyber Dialogue, *Online Privacy Issues Divide Internet Users,* <http://biz.yahoo.com /prnews/000420/ny_cyber_d_1.html> (accessed Apr. 20, 2000) (noting an April 2000 survey found that 69% of Internet users had unknowingly signed up for e-mail distribution lists, 40% did not know what cookies were or how they worked, and 21% were not sure how their browsers were set when it came to cookies); *IBM-Harris Multi-National Consumer Privacy Survey* <http://www.ibm.com/services/files/privacy_survey_oct991.pdf> (accessed Aug. 28, 2000) (noting a recent IBM-Harris multi-national consumer survey showed that 94% of American, 79% of British and 72% of German respondents were concerned about the possible misuse of the personal information online; 61% of American, 39% of U.K. and 49% of German Internet users had refused to purchase goods online because of privacy concerns encompassing a range of issues; 78% were concerned about identity theft, 74% about profiling, 72% about the sale of their personal information, and 65% about the tracking of personal surfing habits across the Web); *see also* Pew Internet & Am. Life <http:// www.pewinternet.org/reports/toc.asp?Report=19> (accessed Aug. 28, 2000) (noting an August 2000 survey by the Pew Internet and American Life Project that 86% of Internet users are concerned about businesses or people they don't know getting personal information about themselves or their families and 54% say they are "very concerned" and 46% are not confident that their online activities are private).

8. *See infra,* nn. 96-117.

9. *Id.*; *Electronic Privacy Information Center v. Federal Trade Commission,* <http:// www.epic.orgprivacy/litigation/> (accessed Aug. 28, 2000) (explaining that the Electronic Privacy Information Center has filed suit in federal district court in Washington seeking the disclosure of records of privacy complaints received by the Federal Trade Commission). It is EPIC's contention that the FTC has failed to take action on the many privacy complaints that the agency has received from consumers. *Id.* In order to evaluate the effectiveness of the current privacy system in the United States, EPIC says it is critical to look at how the FTC responds to complaints from the public. *Id.* EPIC filed the initial information request on June 10, 1999. *Id.*

10. *See infra,* nn. 146-151. After the European Commission decided in March 2000 that the U.S. safe harbor proposal provided an "adequate level of protection" to permit transborder data flows to compliant U.S. companies under Article 25 of the European Directive, the European Parliament voted in a July 5, 2000 resolution to express the view that the arrangement needed to be improved in the area of remedies for individuals in case of breaches of its principles. *Id.* The Commission decided to go ahead with the its March 2000 decision and put the U.S. Department of Commerce on notice that it would re-open discussions to seek improvements if the Parliament's fears proved to be well-founded. *Id.*; *see also* The European Commission, *European Commission's Statement on Safe Harbor Agreement* <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm> (July 27, 2000).

11. The Center for Democracy and Technology, *Summary of Major Consumer Internet Privacy Bills in the 106th Congress, Privacy Legislation Information Forum* <http://www.

pending legislation touches on sectoral privacy issues without being Internet specific.[12] The bipartisan nature of these proposals and their persistence on the legislative agenda is perhaps the most profound indicator of the widely perceived need for some form of government regulation. Yet fears that state intervention will stifle e-commerce growth have animated stark disagreement on these issues within Congress and among members of the Federal Trade Commission.[13]

Proponents of self-regulation challenge the bedrock assumptions underlying calls for online regulation: they dispute that online businesses abuse their power to collect and use information and that profit incentives conflict with privacy interests.[14] Consumers ultimately control their privacy choices on the Internet; and when they express privacy concerns, market forces respond by introducing new mechanisms like web seal programs and privacy enhancing technologies which "could eventually quell privacy concerns altogether."[15] Government intervention would smother this process, harm consumers by denying them product flexibility, and hinder electronic commerce by raising start-up and other costs of online businesses.[16] Consumer education and industry self-regulation, with the help of Federal Trade Commission oversight to prevent fraudulent and deceptive practices, would permit e-commerce to harness the profit incentives already driving businesses to protect consumer pri-

---

cdt.org/legislation/106th/privacy/> (accessed Nov. 16, 2000) (containing a complete list and brief summary of these bills); *see also Consumer Privacy Protection Act*, Sen. Res. 2026, 106th Cong. 2000; *The Privacy Commission Act*, H.R. Res. 4049, 106th Cong. (2000) (supplying two examples of comprehensive regulatory schemes that would be set up to establish a temporary representative stakeholder agency to examine a broad range of privacy issues including the need for Internet regulation and the effectiveness of self-regulation).

12. *Id.*; *Electronic Signatures in Global and National Commerce Act*, H.R. Res. 1714, 106th Cong. (2000) (noting the search for regulatory solutions has also been accelerated by the introduction in Congress of e-commerce and digital signature legislation, which itself calls for some measure of consumer protection).

13. *See generally* Federal Trade Commission, *How to Be Web Ready* <http://www.ftc.gov/bcp/conline/pubs/online/webready/index.htm> (accessed Nov. 11, 2000).

14. *E.g.*, Justin Matlick, *Governing Internet Privacy: A Free-Market Primer*, Pacific Research Institute <http://www.pacificresearch.org/issues/tech/intpriv/main.html> (accessed Aug. 28, 2000).

15. *Id.*

16. *Id.* (explaining Pacific Research also argues that regulations would erode the protections provided in the U.S. Constitution by upsetting the delicate balance between the competing interests of privacy and free expression and, at the same time, "erode the sense of freedom, responsibility, and accountability that prevails on the World Wide Web."). "The best policy would avoid regulation and instead harness the profit incentives already driving businesses to protect consumer privacy." *Id.* "Such an approach would help consumers safeguard their privacy, protect the freedom and enterprise that underline the Internet's promising future, and ensure that the Constitution remains intact." *Id.*

vacy, and should be given time to work.[17]

Other policy analysts question whether business forces and technological innovation alone can keep pace with the growing demands of consumers, legislators, and other nations for adequate and consistent privacy rules.[18] Vastly different business and technology "solutions" create a confusing and frequently misleading array of levels of "protection" and privacy "choices" which can actually impede the development of consumer trust online and the capacity for growth in e-commerce industries. Privacy concerns cannot be resolved by browser design features that simply permit users to accept or reject "cookies," or by the voluntary adoption of privacy policies by a comparative handful of the tens of thousands of Web sites that collect personal information globally. If they exist at all, many privacy policies are extremely limited in scope, more honored in their breach, or readily circumvented by data tracking technologies which offer Internet users no choice at all in the collection, use or dissemination of their personal data.[19] These problems are magnified in a

17. *Id.*; *see also* Roscoe B. Starek, III & Linda Rozelle, *The Federal Trade Commission's Commitment to Online Consumer Protection*, 15 John Marshall J. Computer & Info. L. 679, 697 (1997).

18. Joel R. Reidenberg & Paul M. Schwartz, *Data Protection Law and On-Line Services: Regulatory Responses*, <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/studies/regul.pdf> (accessed Aug. 28, 2000) (noting that this study was prepared as part of the project "Vie privée et société de l'information: Etude les problèmes posés par les nouveaux services en ligne en matière de protection des données et de la vie privée" commissioned from ARETE by Directorate General XV of the Commission of the European Communities 144-153 (1998)); *see also* Joel R. Reidenberg, *International Data Transfers and Methods to Strengthen International Co-operation* <http://home.sprynet.com/~reidenberg/idt.htm> (accessed Aug. 24, 2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L.J. 1607, 1609, 1685 (1999); Sen. Commerce Comm., *Hearings on Internet Privacy and Profiling*, statement of Marc Rotenberg, 106th Cong. <http://www.epic.org/privacy/internet/senate-testimony.html> (accessed Aug. 28, 2000).

19. Christopher D. Hunter, *Recoding the Architecture of Cyberspace Privacy: Why Self-Regulation and Technology Are Not Enough*, <http://www.asc.upenn.edu/usr/chunter/net_privacy_architecture.html> (accessed Jan. 1, 2000) (noting that online consumers are both distrustful and confused by online privacy policies). One study indicated that 64% of respondents were unlikely to trust a Web site regardless of whether or not it posts a privacy policy. *Id.*; *see also* Steve Lohr, *Survey Shows Few Trust Promises on Online Privacy* in *The New York Times* (Apr. 17, 2000) (available in 2000 WL 21240456(1)) (reporting a survey by Odyssey that indicated that 92% of online households agreed or agreed strongly with the statement: "I don't trust companies to keep personal information about me confidential, no matter what they promise"); Will Rodger, *Privacy Isn't Public Knowledge, Online Policies Spread Confusion with Legal Jargon*, in USA Today (available at <http://www.usatoday.com/life/cyber/tech/cth818.htm>) (accessed May 2, 2000) (reporting that online privacy policies conducted for USA Today found that "without exception, policies are ponderous, full of jargon or written so as to leave many surfers scratching their heads."). This analysis included sites certified by seal programs such as TRUSTe. The Yahoo! policy, as an example, had 3,405 words and 167 sentences. *Id.* In DoubleClick's policy, a user had to read through over 2,000 words, on three different pages, before they came to the opt-out provisions. *Id.*

global environment where differing national rules can disrupt international data flows to countries that do not offer adequate protections.[20] Legislated and binding international standards, it is argued, are the only effective means available to address these concerns.[21]

Assuming some form of state regulation is necessary, there remains the question of oversight and enforcement. Should the U.S. adopt a traditional regulatory model under which the FTC and sector specific agencies would assume administrative oversight? Should civil remedies be available to aggrieved individuals? Should a new "Privacy Czar" be established to set standards and oversee their implementation and enforcement? Is there a place for self regulation within any of these models?

This paper presents a snapshot of current issues and imperatives for online regulation. It argues that the U.S. should adopt a privacy regime modeled on widely accepted fair information practices for both online and conventional data processing activities. It calls for oversight responsibilities to be assigned to a single specialized agency that can mediate appropriate standards across a broad range of business contexts and technologies. Finally, it invites this new U.S. Privacy Commissioner to join the dialogue now underway among the data protection officials of other nations to resolve the complex issues of privacy policy implementation presented by information technologies of global reach.

II. THE EXISTING REGULATORY FRAMEWORK

The use of regulatory instruments for protecting privacy rights in the U.S. is not a new phenomenon. The development of centralized databases in the 1960's and 1970's raised the specter of creeping state surveillance and led to the adoption of laws and codes to ensure that governments and other monolithic organizations recognized individual privacy rights and assumed commensurate responsibilities to protect personal data.[22] Many nations extended protections to government data holdings, and in some cases to the private sector, while industry and professional associations voluntarily adopted codes of conduct.[23] The U.S. Privacy Act of 1974[24] was one of the first national measures to implement fair information practices governing the personal data processing activities of federal government agencies.[25] These comprehensive rules

20. Schwartz, *supra* n. 18, at 1701-1702.

21. *Id.*

22. *Omnibus Crime Control & Safe Streets Act*, Pub. L. No. 90-351, 82 Stat. 236 (1994).

23. Philip E. Agre, *Introduction, in Technology and Privacy, The New Landscape* 2 (Philip E. Agre & Marc Rotenberg, MIT Press 1998).

24. *Privacy Act*, 5 U.S.C. § 552 (1994).

25. *Id.*

quickly earned international recognition and were adopted in 1980 by the Organization for Economic Co-operation and Development in Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines).[26] These same rules are the foundation of data protection legislation around the world today, as well as industry privacy codes, online privacy seals, and individual privacy policies.[27]

---

26. Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM> (accessed Nov. 17, 2000) [hereinafter "OECD Guidelines"].

27. *Id.*; OECD Guidelines: Part Two. *Basic Principles of National Application*, supra n. 26.

> *Collection Limitation Principle:*
> 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
> *Data Quality Principle*
> 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
> *Purpose Specification Principle*
> 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
> *Use Limitation Principle*
> 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
> a) with the consent of the data subject; or
> b) by the authority of law.
> *Security Safeguards Principle*
> 11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
> *Openness Principle*
> 12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
> *Individual Participation Principle*
> 13. An individual should have the right:
> a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
> b) to have communicated to him, data relating to him:
> within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
> c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
> d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
> *Accountability Principle*
> 14. A data controller should be accountable for complying with measures, which give effect to the principles stated above.

Id.

Additional U.S. privacy laws governing the private and public sector have been enacted in response to new technologies or uses of sensitive information that have raised public concerns and called for the creation of specific standards.[28] The *Fair Credit Reporting Act* (*FCRA*) is one of the more comprehensive laws incorporating basic fair information practices, including limits on the collection, use and disclosure of information, and rules for access and correction.[29] The *FCRA* provides for administrative oversight by the FTC under the deceptive and unfair practice provisions of the Federal Trade Commission Act,[30] sector specific oversight by other regulatory agencies, and civil remedies in the courts for aggrieved individuals.[31] Other statutes provide more limited protections and enforcement tools. Video privacy laws prohibit the disclosure of sales and rental records and provide only for civil remedies in the courts.[32] A broader range of rules governs cable service providers in the collection, use, disclosure, retention, and access rights for information collected from cable subscribers, including strong notice requirements.[33] Cable and telephone subscribers are both given limited civil rights of action to remedy violations; but laws protecting telephone subscribers from unsolicited telemarketing schemes also extend civil rights of action to each state and regulation-making and court intervention authority to the Federal Communications Commission.[34] Financial records are protected from improper collection and disclosure by federal agencies and financial institutions.[35] Customers of financial institutions have civil remedies for breach of their rights; and the federal government is given disciplinary responsibilities where a court determines that any violation by a federal employee has been willful.[36] State motor vehicle

28. *Privacy Act*, 5 U.S.C. § 552 (1994); *Fair Credit Reporting Act*, 15 U.S.C. §§ 1681-1688t (1994); *Freedom of Information Act*, 5 U.S.C. § 552 (2000); *Family Educational Rights and Privacy Act*, 20 U.S.C. § 1232g (1994); *Right to Financial Privacy Act*, 12 U.S.C.S. § 3412 (2000); *Privacy Protection Act*, 42 U.S.C. § 2000aa (2000); *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1848-73 (1986); *Video Privacy Protection Act*, 18 U.S.C. § 2710 (1994); *Employee Polygraph Protection Act*, 29 U.S.C.S. §§ 2001 *et seq.* (2000); *Cable Communications Policy Act of 1984*, 47 U.S.C. § 551 (2000); *Telephone Consumer Protection Act*, 47 U.S.C.S. § 222 (2000); *Drivers' Privacy Protection Act*, Pub. L. No. 103-322; 108 Stat. 1796 (1994); *Financial Services Modernization Act*, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

29. *Fair Credit Reporting Act*, 15 U.S.C. §§ 1681n (1994).

30. *Federal Trade Commission Act*, 15 U.S.C. § 45(a) (2000).

31. *Fair Credit Reporting Act*, 15 U.S.C. §§ 1681n, 1681o, 1681s (1994).

32. *Video Privacy Protection Act*, 18 U.S.C. § 2710(c) (1994).

33. *Cable Communications Policy Act*, 47 U.S.C. § 551(f) (2000).

34. *Id.*; *Telephone Consumer Protection Act*, Pub. L. No. 107-5, 47 U.S.C. §§ 227(c), 227(f) (2000).

35. *Financial Services Modernization Act of 1999*, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

36. Pub. L. No. 106-102, 113 Stat. §§ 3416-3418.

records are subject to the disclosure provisions of the *Driver's Privacy Protection Act* with no specific enforcement mechanisms or oversight.[37] Other laws fall somewhere among the protection levels and enforcement mechanisms afforded by these examples.

Over the last 25 years the *Privacy Act of 1974* and the patchwork of protections provided by other record specific laws have suffered from criticisms of their effectiveness for protecting privacy rights.[38] Their shortcomings have been attributed to three main sources: new and unanticipated uses of digital data (i.e., other than for the purposes for which it was originally collected); the inconsistent application of similar privacy rules by different record keepers; and, most significantly, the lack of effective oversight and uniform enforcement.[39] It is no coincidence that

37. *Drivers' Privacy Protection Act*, Pub. L. No. 103-322; 108 Stat. 1796 (1994);

38. Colin Bennett, *Convergence Revisited, Does Privacy Law Work, Technology and Privacy, The New Landscape, Introduction* 113 (Philip E. Agre & Marc Rotenberg, ed., MIT Press 1998); *see also* Robert Gellman, *Does Privacy Law Work, in Technology and Privacy, The New Landscape, Introduction* 195-202 (Philip E. Agre & Marc Rotenberg, ed., MIT Press 1998).

39. Gellman, *supra* n. 38 at 195-202 (noting that it is not the point of this paper to make the empirical case for the existence of deficiencies). However, the diffuseness of protections and the inconsistencies in oversight mechanisms logically contribute to a less than robust "culture of privacy" in the American political consciousness. *Id.* Gellman argues that the *Privacy Act of 1974* is plagued by serious shortcomings in administration and enforcement provisions in relation to each of the OECD's principles of fair information practices. *Id.* The first of these, the openness or "transparency" principle, which mandates no secret record keeping, has fallen into disrepute due to the lack of any effective oversight mechanism over agencies responsible for maintaining and reporting their personal data records systems. *Id.* While the second principle of individual "participation" has seen many data subjects successfully secure access to and correction of their own personal information, the lack of effective oversight has also undermined the objectives of the third and fourth principles. *Id.* Limits on the collection of personal information and the requirement that it be "relevant, accurate and timely" in light of the purpose for which it is used suffer from the absence of meaningful and consistent guidelines. *Id.* Gellman further notes that the Office of Management and Budget devotes more resources to administering the *Paperwork Reduction Act* than it does to the government's collection responsibilities under the *Privacy Act*. *Id.* Limitations on the internal use of personal information by the record keeper, the fifth or "need to know" principle, suffers from the fact that it is not limited in any way by the purpose for which the information was originally collected, and the principle administrative oversight of "self-serving assessments" made by agency officials. *Id.* The sixth principle which prohibits non-consensual use or disclosure, except for the purpose for which the data was originally collected, has been rendered largely ineffective by the lack of clear definition of the agency's purpose or purposes at the time of collection, and the fact that these purposes are constantly shifting as new or so-called "routine uses" are identified. *Id.* The statute's requirement for the publication of a notice in the Federal Register has become the only procedural hurdle in the face of bureaucratic expedience. *Id.* Most significantly, cross-agency computer matching programs used to detect social welfare and other types of fraud are also departures from the purposes for which many personal records were originally collected. *Id.* The *Computer Matching and Privacy Protections Act of 1988* has produced some procedures, but few, if any, substantive changes to federal com-

these shortcomings reflect parallel concerns about online privacy rights and the efficacy of any regulatory regime for securing their protection. Driven by market and profit incentives, online businesses have maximized the amount of personal information they collect, and without notice, have used it for purposes consumers never contemplated.[40] Online data protection rules are inconsistent at best, and frequently non-existent. Where they do exist, whether under voluntary privacy policies or self-regulatory instruments, their effectiveness is entirely dependent on the mechanisms available to implement and enforce them, which are largely missing in the online world.[41] It is not unreasonable to observe that the proponents of any regulatory model which aspires to protect online privacy must first recognize and be prepared to correct the shortcomings identified in existing rules or laws.

---

puter matching programs. *Id.* The seventh and eighth principles enshrined in the *Privacy Act* are security and accountability of those responsible for administering the *Act*. *Id.* These principles ensure appropriate administrative, technical and physical safeguards for information protection, but are subject to the vicissitudes of hacking and human error. *Id.* The absence of uniform standards and oversight in the U.S. has compounded these risks. *Id.* Moreover, the threat of civil and criminal penalties as a deterrent to non-compliance has diminished dramatically as administrators have became familiar with the weaknesses in the law while the bureaucratic stomach for enforcement or prosecution has diminished. *Id.* Individual lawsuits seeking damages and injunctive relief are severely limited by law, prompting one official to describe the *Act* as "largely unenforceable" by individuals. *Id.*

40. Judiciary Committee, Subcommittee on Courts and Intellectual Property, statement of Jerry Berman, Executive Director, Center for Democracy and Technology, <http://www.cdt.org/testimony/990527berman.shtml> (May 27, 1999) (noting that the Internet accelerates the trend toward increased information collection already evident in the offline world). The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. *Id.* When aggregated, this data can reveal an enormous amount about personal lives. *Id.* This increasingly detailed information is bought and sold as a commodity by a growing assortment of players and often sought by governments. *Id.*; *see also* Schwartz, *supra* n. 18, at 1609, 1689-1690.

41. Robert Gellman, *Conflict and Overlap in Privacy Regulation: National, International and Private* <http://www.ksg.harvard.gov/iip/glisony/gellman.html> (accessed Apr. 7, 2000) (stating that broad agreement on general principles such as those reflected in the OECD Guidelines are not enough to establish the common processes and procedures needed to implement and enforce common international privacy rules). Gellman points to the experience in the United States regarding implementation of the OECD Guidelines to illustrate the practical shortcomings of general standards. *Id.* Many companies have agreed to the standards, but few have changed their practices or policies. *Id.* He further argues that there should be substantive and procedural details that go beyond general principles. *Id.* In particular, there should be an enforcement mechanism that offers some oversight of the activities of record keepers as well as a practical remedy for individuals. *Id.; see also* The European Commission, *Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp7en.htm> (accessed Nov. 17, 2000) (discussing the European Working Party's views on the minimum content of adequate enforcement mechanisms in a self-regulatory context).

III. SELF-REGULATION VERSUS STATE REGULATION IN THE 106TH CONGRESS

Important and innovative measures have been pursued on a variety of non-regulatory and self-regulatory fronts to enhance consumer privacy and confidence on the Internet. In addition to industry privacy codes, Web seal programs have the potential to foster greater consistency in Internet privacy policies and encourage consumer confidence in e-commerce.[42] Electronic commerce and consumer protection groups have developed standards and guidelines for business to consumer transactions.[43] Online resources exist to help businesses implement and

42. *E.g.*, TRUSTe, *TRUSTe Approves 1000th Web Site: Internet Industry Rallies Around TRUSTe Privacy Seal as Prominent Symbol of Trust Online,* <http://biz.yahoo.com/prnews/000112/ca_truste__1.html> (Jan. 12, 2000) (announcing in January it had awarded its 1,000th Privacy Seal); *Id.* (offering the WebTrust Seal; Germany joined England, France, Scotland, Ireland and Wales in the European Union in offering WebTrust Seal; WebTrust is also available in Australia, Canada and Puerto Rico, in addition to the United States); WebTrust, *AICPA'S WebTrust Seal of Assurance Expands Into France, Joining Other EU, Asia-Pacific and North American Countries to Protect Online Privacy and Shopping* <http://biz.yahoo.com/bw/000119/ny_aicpa_1.html> (Jan. 19, 2000); Business Wire, *New Online Privacy Protection Tool to Transcend Borders* <http://www.businesswire.com/webbox/bw.051800/201391381.htm> (May 18, 2000); The Good Housekeeping Web Site Certification <http://www.gh-atyourservice.com/certificate/prog_info.html> (May 19, 2000).

43. *E.g.,* Council for Internet Commerce, *Council Approves Final Standard for E-Commerce* <http://biz.yahoo.com/rf/991214/bf0.htm> (Dec. 16, 1999) (according to the Council, it specifies the merchant practices and policies that lead to high levels of customer satisfaction, service, security and privacy); The Standard, *E-commerce Sites Move Towards Code of Conduct* <http://thestandard.com/article/display/0,1151,7229,00.html> (Oct. 27, 1999); The Standard, *The Standard for Internet Commerce* <http://www.gii.com/standard/about.html> (accessed Nov. 10, 2000); The Standard, *What is the Standard for Internet Commerce* <http://www.gii.com/standard/faq/aboutsic.html#whatis> (accessed Nov. 10, 2000); PricewaterhouseCoopers, *Global Business Dialogue Finalizes Policy on Protection of Personal Data*, <http://www.pwcbetterweb.com/betterweb/AboutSeal/seal_std.cfm> (accessed Aug. 28, 2000) (stating that the Global Dialogue for Electronic Commerce, a consortium of companies formed to "strengthen international coordination of e-commerce rules," finalized its policy on the protection of personal data"); Electronic Commerce and Consumer Protection Group, *Internet and E-Commerce Group Proposes Guidelines for Consumer Protection Online* <http://www.Ecommercegroup.org/press.htm> (June 7, 2000) (stating that at the beginning of June 2000, the Electronic Commerce and Consumer Protection Group, made up of America Online, AT&T, Dell, IBM, Microsoft, Network Solutions and Time Warner, proposed *Guidelines for Merchant-to-Consumer Transactions* and a companion *Statement on Global Jurisdiction Framework for Electronic Commerce*). The guidelines also include a section on privacy protection. *Id.;* Privacy Leadership Initiative, *Industry Leadership Group to Tackle Privacy Concerns; Privacy Leadership Initiative Focuses on Consumers' Concerns About Privacy and Offers Rapid Work Plan* <http://biz.yahoo.com/prnews/000619/dc_privacy.html> (June 22, 2000) (stating that in June 2000, a group of more than 20 corporate CEOs and trade association executives announced the formation of the Privacy Leadership Initiative (PLI)). Members of this alliance include Procter & Gamble, IBM, Ford, Intel, Sony, E*TRADE, and AT&T. *Id.* Among other initiatives, the PLI plans to: (a) perform an analysis of currently available privacy technologies, identify capability gaps

consumers recognize smart data protection practices, with information on opt-out/opt-in choice, privacy organizations, legislative and legal resources, privacy policy generators, seal programs, cookies, web bugs, encryption, and related surveys.[44] Individual companies have created new privacy enhancing technologies (PET's) for anonymization, pseudonymization, infomediation, and encryption, giving Internet users additional tools for controlling privacy choices.[45] Newer PET's could soon permit users to access and change their existing online profiles on Websites powered by particular technology developers.[46] When finalized, the World Wide Web Consortium's Platform for Privacy Preference project (P3P) could emerge as an international and industry standard providing automated ways for users to gain more control over the collection and use of personal information on Web sites visited.[47] All of these

---

and offer ways to make these technologies broadly available to individuals; (b) conduct consumer research to understand specifics of consumer privacy concerns and to provide a baseline for measuring progress; (c) design a set of online privacy templates that enable companies to efficiently implement appropriate privacy practices and conduct an outreach campaign to assure broad distribution in industry; (d) conduct a consumer education campaign to address consumers' concerns and inform consumers of technology efforts that allow them to control their own privacy; and (e) form a private sector-led forum, independent of the initiative, that will conduct ongoing and informed assessments of privacy policy issues, and inform stakeholders of its recommendation. *Id.*

44. *See e.g.* Electronic Commerce and Consumer Protection Group, *Internet and E-Commerce Group Proposes Guidelines for Consumer Protection Online* <http://www.ecommercegroup.org/press.htm> (June 6, 2000). Enonymous.com runs a Web site (http://www.privacyratings.org) where anyone can check the privacy policy and enonymous.com's rating of 30,000 of the most popular Web sites. *Id.* In May 2000, Privacy Council, Inc. launched a Web site (http://www.privacycouncil.com) designed to help business implement and consumers recognize "smart privacy and data practices." *Id.*; Privacy Council, Inc., *Leading Privacy Company Launches Most Comprehensive Interactive Web Site On Internet* (May 4, 2000) <http://www.privacycouncil.com/> (June 06, 2000) (providing current resources information and links regarding opt-out, privacy organizations, legislative and legal resources, privacy policy generators, seal programs, cookies, encryption, infomediaries, and related surveys).

45. *See e.g.* Companies such as Anonymizer.com, Zero Knowledge Systems, Lumeria Network with its PrivacyPlace Web site, Novell's digitalme, Privaseek's Persona, e-DENTIFICATION, @YourCommand, nCognito, and Lucent Personal Web Assistant.

46. Kenneth Hein, DM News, *Online Marketers Open Up the Profile Files to Consumers* <http://www.dmnews.com/articles/2000-08-07/9872.html> (Aug. 11, 2000) (providing examples: BrightStreet & BrandStamp).

47. Ann Cavoukian, Michael Gurski, Deirdre Mulligan, Ari Schwartz, *P3P and Privacy: An Update for the Privacy Community* <www.cdt.org/privacy/pet/p3pprivacy.shtml> (Mar. 28, 2000) [hereinafter *P3P and Privacy*]. This technology employs a standardized set of multiple-choice questions, covering all the major aspects of a P3P enabled Web site's privacy policies. *Id.* P3P enabled browsers can automatically "read" how a site handles personal information about its users and compare it to the consumer's own set of privacy preferences, enabling users to act on any inaccuracies. *Id.* While the P3P initiative is subject to certain limitations—for example, it cannot ensure that companies follow privacy policies—the standardization in transparency and choice that it offers and its adaptability

initiatives suffer from the common defect that they cannot ensure companies follow privacy policies. None conform to the fundamental OECD principle that it is the data controller, and not the data subject, who is responsible for complying with practices, which provide a minimum and non-negotiable level of protection for all individuals.[48] Nonetheless, many may prove useful in implementing fair information practices across a broad range of business contexts and regulatory responses.

Technological developments and the growing information-based economy have prompted government, consumers' associations, industry groups and academics in the U.S. to re-examine existing public policy and consider new regulatory initiatives. A 1998 Federal Trade Commission report called for legislation to protect children's personal data collected over the Internet, and recommended a legislative response to adult online privacy issues if self-regulatory efforts did not improve levels of protection within the next year.[49] At the same time the U.S. Administration announced initiatives for an Electronic Bill of Rights[50] supporting additional measures in the areas of medical and financial data and identity theft, but otherwise encouraging self-regulation as a means of permitting e-commerce to flourish.[51]

The Childrens' Online Privacy Protection Act of 1998 ("COPPA")[52] is the first and, to date, the only U.S. law specifically geared toward online privacy protection. *COPPA* requires that commercial Websites directed to children[53] post privacy policies, obtain parental consent, and observe

---

to add-on products, such as anonymizers, makes it a potentially useful tool for implementation of either voluntary codes or legislated public policy initiatives. *Id.*

48. The European Commission, *Platform for Privacy Preferences and the Open Profiling Standard* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp11en.htm> (accessed Aug. 28, 2000); *see also* Schwartz, *supra* n. 16, at 1609, 1695-96. "P3P has great potential to assist in the customization of individual wishes for information privacy." *Id.* "The difficulty, as already noted in the context of infomediaries, is that a lock-in of a poor level of privacy is likely to occur around a norm of maximum information disclosure." *Id.* "By itself, P3P will not cause change in the existing norm of maximum disclosure. Rather, Web sites will be able to use P3P to close themselves off to individuals who seek the fair information practices that I have proposed." *Id.* "In other words, those who view the Internet through the filter of privacy-enforcing software may end up placing most of the Web off limits to themselves." *Id.* "Their Hobson's choice will be sacrificing either their privacy or their access to the Internet." *Id.*

49. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* <http://www.ftc.gov/reports/privacy3/index.htm> (July 1998).

50. Office of the Vice-President, *Vice President Al Gore Announces New Steps Towards an Electronic Bill of Rights* (July 31, 1998) (copy on file with the author).

51. Schwartz, *supra* n. 18, at 1609, 1611, 1639-40, nn. 8, 199-205 (reviewing the Clinton Administration's approach to online privacy protection and self-regulation. *Id.*

52. *The Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§ 6501-6506 (1999).

53. 15 U.S.C. § 6501(a) (stating that the *Act* also applies to other sites that knowingly collect personal information from children).

rules governing the collection, use, disclosure and security of children's personal information under regulations promulgated by the FTC.[54] Like the *FCRA*, *COPPA* gives administrative oversight to the FTC and other sectoral agencies, and it provides for state enforcement in the courts, but not for individual rights of action.[55] *COPPA* also experiments with self-regulation in the form of "safe harbor" rules or "self-regulatory incentives." Under these rules, Web site operators will be deemed to be in compliance with the FTC's implementing regulations if they follow a set of self-regulatory privacy guidelines developed by industry representatives,[56] which must first have been published for comment and approved by the FTC.[57] The delayed implementation of *COPPA* pending the development of FTC regulations[58] has left the U.S. without the benefit of experience to measure the law's effectiveness in the online world.[59] Yet, in this one area at least, Congress and the Administration have accepted that online privacy is amenable to regulation, employing the complete range of fair information practices adapted to specific industries by accommodating their approaches to self-regulation.

Two of the many bills currently before Congress, one in the House and one in the Senate, illustrate the range of legislative responses available for further regulatory initiatives. Bill H.R. 4049 is an act "To establish the Commission for the Comprehensive Study of Privacy Protection."[60] The findings in the bill speak to the gravity and complexity of the issues confronting America: the growing concern about civil liberties and the use and security of personal data; the pressures on commercial entities to adopt privacy policies; specific concerns about sensitive data such as medical and financial information, and Social Security Numbers; the growth of the Internet and e-commerce at an "astounding rate"; reports of "surreptitious collection" and "questionable redistribution" of personal data; the leading role of America in the global information economy; the mounting pressures of international standards; and

54. 15 U.S.C. § 6502(b).

55. 15 U.S.C. §§ 6504-6506.

56. 15 U.S.C. § 6503(a).

57. 15 U.S.C. § 6503(b); *see also* The DMA Interactive, *How to Comply With The Children's Online Privacy Protection Rule* <http://www.the-dma.org/library/privacy/children.shtml> (accessed Aug. 28, 2000) (stating that as this paper went to print, for example, the Direct Marketing Association published an online a guide and privacy policy generator designed to help direct marketers comply with *COPPA* and the FTC rules). The FTC had not yet published the policy for comment and approval. *Id.*

58. 15 U.S.C. § 6503.

59. 15 U.S.C. § 6506; *see also* The DMA Interactive, *supra* n. 57. The FTC is to report to Congress in 5 years on *COPPA*'s effects on the ability of children to obtain access to information of their choice online and on the availability of Web sites directed to children. *Id.*

60. *The Privacy Commission Act*, H.R. Res. 4049, 106th Cong. (2000).

the need to reassess the most effective way to balance privacy and information uses in light of possible unintended effects on technology development, innovation, the marketplace, and privacy needs.[61] Bill H.R. 4049 proposes the creation of a bipartisan 17 member Commission to study and report within 18 months on issues relating to privacy protection and the appropriate balance to be struck between protection and permissible uses of information.[62] The study would be exhaustive. It would encompass personal data processing by federal, state, and local governments, and private entities, including automated and Internet transactions. It would also assess current efforts to address privacy issues including existing statutes and regulations, pending legislation, and other efforts undertaken by the federal, state, and foreign governments, international bodies, and the private sector.[63] The final report would make detailed findings and recommendations in all of these areas, including the effectiveness of self-regulatory efforts, technology advances, and market forces in protecting individual privacy; whether additional legislation is necessary, and if so, specific proposals to reform or augment current laws; the extent to which additional regulations may impose undue costs or burdens, or cause unintended consequences in other policy areas, such as security, law enforcement, medical research, or critical infrastructure protection; cost-benefit analyses of any legislative or regulatory changes proposed; and recommendations on non-legislative solutions, including education, market-based measures, industry best practices, and new

61. *Id.* at § 2.

"Americans are increasingly concerned about their civil liberties and the security and use of their personal information . . . [and] . . . [c]ommercial entities are increasingly aware that consumers expect them to adopt privacy policies and take all appropriate steps to protect personal information of consumers. There is a growing concern about the confidentiality of medical records, because there are inadequate Federal guidelines and a patchwork of confusing State and local rules regarding privacy protection. [R]ecent changes in financial services laws allow for increased sharing of information between traditional financial institutions and insurance entities. The use of Social Security numbers has expanded beyond the uses originally intended. Use of the Internet [and] [f]inancial transactions over the Internet have increased at an astounding rate [and] as a medium for commercial activities will continue to grow. There have been reports of surreptitious collection of consumer data by Internet marketers and questionable distribution of personal information by online companies. The United States is the leading economic and social force in the global information economy, largely because of a favorable regulatory climate and the free flow of information. The shift from an industry-focused economy to an information-focused economy calls for a reassessment of the most effective way to balance personal privacy and information use, keeping in mind the potential for unintended effects on technology development, innovation, the marketplace, and privacy needs."

Id.

62. *Id.* at § 5.

63. Richard Lauter, *Privacy Concerns and Safeguards in the Governmental Dissemination Data of Bankruptcy Data on the Internet*, 2000 ABI JNL.LEXIS 49.

technologies.[64]

A significant feature of bill H.R. 4049 is that it is not confined to issues of consumer privacy on commercial Web sites, but opens up for review the full range of existing privacy infrastructures and regulatory measures affecting data processing by all levels of government and the private sector, and deals with conventional off-line practices as well as privacy issues on the Internet. As the first such study in 25 years, it is long overdue.[65] While H.R. 4049 is currently on a fast track through Congress and has been given qualified support by some privacy advocates,[66] critics see it as means of burying the issue under "an avalanche of politics" by surveying once again the views of "grid-locked groups" whose opinions are already "set in stone."[67] They argue that a strong case has already been made and that sufficient studies now exist to move forward on immediate legislation to regulate Internet privacy protection.[68]

One such measure is bill S. 2026, the *Consumer Privacy Protection Act*.[69] The recitals of this *Act* recognize privacy as a "fundamental right worthy of legislative protection" and acknowledge that consumers have an "ownership interest" in their personal information, including the

64. H.R. Res. 4049, 106th Cong. § 4.

65. Jon Sarche, *Privacy To Headline Tech Summit* Washington Post, (Aug. 21, 2000) <http://www.washingtonpost.com/wp-srv/aponline/20000820/aponline130011_000.htm> (reporting Rep. Asa Hutchinson's remarks to Sixth Annual Technology Policy Summit sponsored by the nonprofit Progress and Freedom).

66. Ari Schwartz, Center for Democracy and Technology, *Testimony before the House Comm. on Government Reform, Subcomm. On Government Management, Information and Technology*, H.R. 4049 - *Privacy Commission Act*, 106th Cong., Apr. 12, 2000 <http://www.cdt.org/testimony/000412schwartz.shtml>.

67. Sen. John McCain, Chairman of the Senate Commerce Committee, quoted by Robert MacMillan, *McCain Aims For Privacy Law By Year-End* in *Newsbytes* http://www.newsbytes.com> (July 26, 2000).

68. H.R. Comm. on Government Reform & Subcomm on Government Management, Information & Technology, *Privacy Commission Act Hearings on H.R. 4049*, 106th Cong., (Testimony of Ari Schwartz) available at <http://www.cdt.org/testimony/000412schwartz.shtml> (Apr. 12, 2000). Shwartz stated: "A commission to study privacy could help, but must not be used as an excuse to delay." *Id.* For 30 years, federal commissions have played an active role in shaping privacy in America. We must neither duplicate past work, nor allow a commission to prevent legislation on issues examined by previous commissions from moving forward. *Id.* This is particularly important in the areas of Internet, medical and financial privacy. *Id.*; Martin Stone, Newsbytes, *Privacy Czar Hot Topic At Tech Summit* <http://www.nbnn.com/pubNews/00/153903.html> (Aug. 21, 2000) The bill's sponsor cautions Congress to move slowly in this area, but agrees that industry self-regulation is unlikely to work and that additional legislation may prove necessary: Rep. Asa Hutchinson, R-Ark. remarks to Sixth Annual Technology Policy Summit sponsored by the nonprofit Progress and Freedom. *Id.*

69. *Consumer Privacy Protection Act,* Sen. Con. Res. 2026, 106th Cong. (1999).

right to control how it is collected, used or transferred.[70] Bill S. 2026 would immediately introduce a full range of fair information practices for all online consumer activity. An important component of its protections is that it would require an individual consumer's affirmative consent for any processing activity involving personally identifiable information. It would also extend consent requirements for online processing to information that is not personally identifiable, but on an opt-out basis.[71] Following the familiar U.S. regulatory model, administrative enforcement responsibility would be assigned to the FTC by expanding its jurisdiction over unfair and deceptive practices to include violation of the new online protections, and to various other federal bodies in accordance with existing mechanisms for regulatory oversight.[72] This bill would also create individual and state initiated rights of action.[73] Online rights would be reinforced with whistle-blower protection;[74] and personal information would not be permitted to be sold as an asset in bankruptcy proceedings.[75] Existing protections for video rentals and cable TV subscribers would be extended to books, recorded music, and satellite services.[76] Studies would be authorized to investigate and report on privacy issues associated with e-commerce, the Internet, and the operation of the new Act, as well as off-line consumer privacy issues and employee monitoring in the workplace.[77] Finally, several initiatives would be undertaken to examine, improve upon and develop new computer and Internet security standards and technologies, as well as automated privacy enhancing technologies.[78]

Each of these initiatives is superficially appealing. Current privacy concerns are not confined to users of commercial Web sites, but transcend technologies, conventional data processing activities, and any number of public and private sector contexts.[79] The comprehensive review proposed by H.R. 4049 would examine a broad spectrum of issues and contexts, address shortcomings in existing public and private sector legislation, as well as the new challenges of the Internet and other digital technologies, and examine the role of self-regulation.[80] Bill S. 2026,

70. *Id.*
71. *Id.* §§ 101-103.
72. *Id.*
73. *Id.* §§ 303-304.
74. *Id.* § 305.
75. Sen. Con. Res. 2026 106th Cong. § 601.
76. *Id.* at §§ 201, 631.
77. *Id.* §§ 307, 503.
78. *Id.* §§ 701, 707.
79. The outsourcing and privatization of government and other public services have blurred distinctions between commercial and not-for-profit institutional activities in ways that are not always apparent to users.
80. H.R. Res. 4049, 106th Cong., (2000).

on the other hand, starts from the premise that a compelling case for online consumer protection now exists, and that widely accepted fair information practices provide a technologically neutral framework within which to bring order and standards to this medium.[81] The social and economic costs of regulation, it is argued, will be lower now than if Congress waits until Internet use becomes more prevalent and technologies diverge to the point that standardization of protocols becomes unmanageable.[82] Specific problems should be addressed immediately before a broader review is undertaken to expand on these efforts in other contexts.[83]

IV. SELF-REGULATION VERSUS STATE REGULATION AT THE FEDERAL TRADE COMMISSION

These alternative visions for legislative action parallel even sharper divisions that have emerged in recent FTC reports to Congress dealing with online privacy and profiling.[84] In its June 1998 report, which led to the passage of *COPPA*, the FTC examined the effectiveness of self-regulation, found it lacking, and suggested that *COPPA*-like rules should be expanded to all online consumer activity if self-regulation did not improve privacy performance levels.[85] This report emphasized that enforcement mechanisms providing sanctions for non-compliance were a critical component of any government or self-regulatory program to protect online privacy.[86] In July 1999, the Commission reported some improvement in the frequency and level of disclosure and recommended that industry should be given more time to make self-regulation work.[87]

A May 2000 FTC report supported by 3 out of its 5 members declared that self-regulation had still fallen short of achieving broad-based implementation.[88] The majority recommended that a privacy law gov-

---

81. Sen. Res. 2026, 106th Cong., (2000).

82. Matthew J. Feeley, *EU Internet Regulation Policy: The Rise of Self-Regulation*, B.C. 22 Intl. & Comp. L. Rev. 159 (1999).

83. Sen. Con. Res. 2026 106th Cong. § 2 (13), (14) (2000).

84. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* <http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf> (accessed May 2000) [hereinafter *Fair Information Practices*]; Federal Trade Commission, *Privacy Online: A Report to Congress* <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (accessed Nov. 16, 2000) [hereinafter *Privacy Online*]; Federal Trade Commission, *Online Profiling, Part 2, Recommendations* <http://www.ftc.gov/os/2000/07/onlineprofiling.pdf> (accessed Nov. 16, 2000) [hereinafter *Online Profiling, Part 2*].

85. Computer Lawyer, *New Rule to Protect Children's Online Privacy in Effect*, 36-37 (June 2000).

86. *Privacy Online*, *supra* n. 84.

87. Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (accessed Nov. 16, 2000).

88. *Fair Information Practices*, *supra* n. 84.

erning consumer Web sites not already covered by the *COPPA* was needed at this "critical time in the development of the online marketplace" to permit electronic commerce to reach its full potential and to permit consumers to participate fully in that marketplace.[89] Such a law should guarantee a basic level of privacy comprising the four basic principles of notice, choice, access and security, and should be expressed in general terms and be technologically neutral to accommodate different business contexts and the state of technological development. An "implementing agency" (presumably the FTC) should have authority to promulgate more detailed "reasonable standards" in rules and regulations, but the report stopped short of recommending more specific enforcement powers, and suggested that self-regulatory measures still had a major role to play in securing online privacy objectives.[90] It would seem that the majority contemplated a law modeled on *COPPA,* with agency promulgated standards and safe harbor provisions for self-regulation, but chose not to dictate the precise model that should be adopted in light of the many legislative initiatives before Congress.

In a dissenting statement calling the majority report "embarrassingly flawed," one Commission member disputed all of its findings and recommendations.[91] Survey results, he argued, showed "continued significant progress" in the frequency and quality of privacy disclosures in each of the four areas of notice, choice, access and security, with an even higher measure of progress if the more problematic areas of access and security were not considered.[92] Studies relied on by the majority were flawed in projecting lost e-commerce revenues in the billions of dollars due to consumer privacy concerns. The report failed to consider the additional regulatory cost burdens on e-commerce which could remove products, services, and marginal businesses from the market altogether.[93] The report also failed to credit recent self-regulatory measures, ignored the impact of developments in privacy enhancing technologies, and gave no thought to enforcement or to the flexibility offered by a self-regulatory safe harbor program.[94] The other dissenting member was able to concur that legislation establishing basic notice requirements was warranted, but disagreed that only online, and not off-line, activity should be regulated, as this would put e-businesses at a disadvantage relative to their off-line competitors.[95] While sensitive data or particular uses of infor-

89. *Id.* at ii-iv, 36-38.

90. *Id.*

91. *Id.* (noting the dissenting statement of Commissioner Orson Swindle).

92. *Id.* at 5-7.

93. *Id.* at 12, 15.

94. *Fair Information Practices, supra* n. 84. at 17-20, 25-26.

95. Thomas B. Leary, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* 1, 7, 10 (May 2000).

mation may call for broader protections beyond simple notice (profiling, for example, was described as a "particularly threatening and distasteful" activity), these should be addressed by Congress on a case-by-case basis.[96] Relying on the Commission's expertise in consumer disclosures and the operation of competitive markets, this commissioner felt that the better course would see the FTC actively pursue existing remedies under the FTCA, and encourage consumer education as a means of disciplining market forces to provide preferred levels of protection.[97]

The second FTC Report to Congress, released in two parts in June and July 2000, specifically addressed the issue of online profiling by network advertising companies.[98] Using "cookies" and "Web bugs,"[99] these companies collect and analyze massive amounts of clickstream data to monitor customers' surfing activities, and then match these with sales data and other demographics to create profiles for target marketing, as well as for sharing with industry partners and sales to other companies.[100] The findings part of the report, which owed much to a public workshop jointly sponsored by the FTC and the U.S. Department of Commerce in November 1999,[101] found that network advertisers engaged in extensive monitoring and collection of personal data for target marketing. Advertisers argued that this activity permitted them to offer consumers preferred products and services, improve their marketing efficiencies and Web site designs, and subsidize free Internet content, among other "benefits."[102] The major concerns expressed with this activity were that it usually took place invisibly without consumers knowledge, that monitoring was extensive and sustained across Web sites and time producing a detailed portrait of individuals' activities, and that the practice was manipulative and deceptive by preying on consumer weakness and creating consumer demand, which would not otherwise exist.[103] Consumer surveys showed overwhelming objections to these practices, even when the information was not made personally identifiable or consumers were given a choice to participate or not.[104]

---

96. *Id.* at 7.

97. *Id.* at 4, 12-13.

98. *Privacy Online*, *supra* n. 84; *see also Online Profiling*, *supra* n. 84.

99. Richard M. Smith, *Web Bug Basics* <www.tiac.net/users/smiths/privacy/wbfaq.htm> (accessed Aug. 28, 2000) Web bugs are tiny and for the most part invisible graphics embedded on a Web page or in an E-mail message. *Id.* The bugs are designed and widely used to monitor who is reading a Web page by sending to the host server the user computer's IP address, the URL of the page the bug is located on, the time it was viewed, the type of browser used, and any previously set cookie value. *Id.*

100. *Online Profiling*, *supra* n. 84, at 3-5.

101. *Id.* at 1.

102. *Id.* at 8-9.

103. *Id.* at 11-14.

104. *Id.* at 15-16.

In Part 2 of its report, the FTC recommended legislation regulating online profiling in terms virtually identical to those used in its May 2000 report, but specifically incorporating safe harbor provisions.[105] Predictably there were dissenting views, with one of the members emphasizing, "We do not have a market failure here that requires legislative solution."[106] The focus of the second part of the report was an accommodation reached with 9 major Internet advertising companies comprising the Network Advertising Initiative (NAI), which coalesced at the same time the Department of Commerce Workshop was taking place.[107] The FTC-NAI accommodation approved a self-regulatory protocol[108] that would provide customers with notice, an "opt-out" choice not to participate in profiling, "reasonable" access to personally identifiable information retained for profiling, status quo security measures,[109] and enforcement consisting of the public reporting of violations and FTC oversight. Notably, opt-in consent would only be required for matching previously collected data with personally identifiable information, or for material changes to a company's processing practices after information had been collected.[110] This latter stipulation was an apparent response to one major advertiser's plans, announced following the Profiling Workshop, to match customers' online surfing habits with other personally identifiable

105. *Online Profiling*, Part 2, *supra* n. 84, at 9-11.

106. *Id.* at 1. Statement of Commissioner Thomas B. Leary Concurring in Part and Dissenting in Part:

> "I agree with the Report's recommendations relating to Online Profiling insofar as they endorse the NAI self-regulatory principles, advocate safe-harbor protections for these principles and others of a similar kind, and recommend some 'backstop legislation.' However, for the reasons expressed in my separate statement relating to online privacy generally, I believe that legislation should focus on adequate 'Notice' and not mandate across-the-board standards for other elements of the so-called 'fair information practices.'"

Id. [The dissenting Statement of Commissioner Swindle provides:]

> My dissent here is not directed to the NAI principles. Rather, it is directed to the majority's recommendation that, despite NAI's laudable self-regulatory efforts, legislation is needed as a 'backstop.' Such legislation would have the same characteristics as the legislation recommended by a majority of the Commission in its 2000 Privacy Report, which I strenuously opposed. Again, the devil is in the details. I consider legislation that mandates the four fair information practice principles to be overly burdensome and unwarranted, for the reasons discussed at length in my dissent from the 2000 Privacy Report. Simply stated, we do not have a market failure here that requires legislative solution.

Id.

107. *Id.* at 4.

108. Network Advertising Initiative, *Self-Regulatory Principles For Online Preference Marketing By Network Advertisers* <http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf> (accessed Aug. 28, 2000).

109. *Online Profiling*, Part 2, *supra* n. 84, at 7–8. The protocol also contained an agreement that NAI members would comply with future security regulations when enacted. *Id.*

110. *Id.* at 6-7.

information.[111] Following a complaint filed with the FTC earlier this year, that plan was temporarily scrapped until an agreement was reached on self-regulatory measures.[112] However, the NAI's FTC-approved policy will now permit personally identifiable profiling in the future unless customers exercise an opt-out choice.

The FTC has said the agreement will give it greater clout to enforce the NAI protocol,[113] but acknowledges that privacy legislation is still needed to ensure that other advertisers also comply with these practices.[114] Advocacy groups have complained about the agreement to the Senate Commerce Committee and Congress,[115] claiming, among other things, that access rights and rights to limit the use of data set out in the FTC-NAI plan are "grossly inadequate," that it "encourages the development of Internet advertising models based on the collection and use of personally identifiable information," and that "the FTC has simply failed to consider adequately the technical and policy implications of profile-based advertising."[116] These concerns are not unfounded. The FTC accommodation with the NAI has effectively preempted the affirmative consent requirement for personally identifiable data processing proposed by bill S. 2026 and has created a compliance model which may prove difficult for Congress to undo once profilers begin to rely on the FTC-sanctioned policy. Unrestricted profiling activity continues among other advertisers and Web sites, which have not attracted FTC attention or the incentives to industry self-regulation, but which also can now call for no less an accommodation from the FTC, and no more onerous regulation from Congress.[117]

---

111. Cheryl Rosen & Beth Bacheldor, *The Politics of Privacy Protection* <http://www.informationweek.com/795/privacy/htm> (accessed July 18, 2000). The company is DoubleClick, which has also recently been defending a class-action lawsuit to stop it from using "Web bugs" to track the minute details of users' Web surfing activities. *Id.*

112. *Id.*

113. Patrick Thibodeau, *Web Advertisers Make Promises on Privacy* <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48413,00.html> (accessed Aug. 28, 2000).

114. *Online Profiling*, Part 2, *supra* n. 84, at 9-11.

115. Electronic Privacy Information Center & Junkbusters, *Network Advertising Initiative: Principles Not Privacy* <http://www.epic.org/privacy/internet/NAI_analysis.html> (accessed Nov. 14, 2000).

116. Electronic Privacy Information Center, *Group Letter on Online Profiling Agreement* <http://www.epic.org/privacy/internet/NAI_group_letter.html> (accessed Nov. 15, 2000); *see also* Electronic Privacy Information Center, *Letter to Senator John McCain About FTC* <http://www.epic.org/privacy/databases/ftc_letter_0797.html> (accessed Nov. 15, 2000); Electronic Privacy Information Center, *Letter to Senate Commerce Committee on NAI* <www.epic.org/privacy/internet/NAI_letter.html> (accessed Nov. 15, 2000).

117. *See e.g.*, Robert O'Harrow Jr., *Firm Tracking Consumers on Web for Drug Companies* <http://www.washingtonpost.com/wp-dyn/articles/A25494-2000Aug14.html> (accessed Aug. 16, 2000). Pharmatrak, a Boston-based technology firm, has been surreptitiously tracking the medical browsing habits of computer users across the Internet on behalf of

The limitations of self-regulation and the efficacy of FTC intervention are illustrated by another recent case triggered by the bankruptcy of a large toy "e-tailer" with a database of family names and personal information on approximately 250,000 customers.[118] Toysmart's Web site displayed a Web seal signifying that it followed fair information practices which, among other commitments, promised that personal information was "never shared with a third party." When the company went into receivership, however, it promptly put its customer database up for sale.[119] The FTC responded to the Web seal administrator's complaint, first by attempting to block the sale in court,[120] but then by reaching a deal that would permit the sale of the list to any prospective buyer in a related market who would agree to abide by the terms of the original privacy policy.[121] In separate bankruptcy proceedings, the court withheld its approval of the deal without an actual buyer on the horizon to give the agreement any substance. While the FTC expressed disappointment that its settlement was rejected, the attorneys general of the 45 states that opposed the deal claimed the court's ruling as a victory for privacy rights, and said that customers should first have been notified and given the opportunity to have their information deleted before any sale was approved.[122] Indeed, in a similar scenario involving a bankrupt

---

major pharmaceutical companies, keeping tabs on when consumers visit web pages maintained by the companies or download information about HIV, prescription drugs, or a company's profits from their various Web sites. *Id.* While Pharmatrak does not currently identify individuals by name, its own Web site suggests it has plans to do so in the future by developing products and services which, "when used in conjunction with the tracking database, could enable a direct identification of certain individual visitors." *Id.* Until recently, at least one participating pharmaceutical company did not post privacy policies on Web sites and new postings still do not mention Pharmatrak. *Id.*

118. Federal Trade Commission, *FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors* <http://www.ftc.gov/opa/2000/07/toysmart.htm> (accessed Aug. 28, 2000). The information included credit card numbers and profiles giving age, gender, names of family children, and their toy preferences. *Id.*

119. Wired News, *Dead Site? There Goes Privacy* <http://www.wired.com/news/business/0,1367,37354,00.html> (accessed Aug. 28, 2000).

120. Federal Trade Commission, *FTC v. Toysmart.com, LLC* <http://ftc.gov/os/2000/07/toysmartcmp.htm> (July 10, 2000). TRUSTe notified the FTC, which in turn filed a complaint in U.S. District Court in Massachusetts charging unfair and deceptive marketing practices in violation of section 5 of the FTC Act and attempting to block the sale. *Id.*

121. Federal Trade Commission, *FTC Announces Settlement With Bankrupt Website Toysmart.com, Regarding Alleged Privacy Policy Violations* <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (July 21, 2000).

122. Stephanie Stoughton, The Boston Globe, *Judge Declines to Rule on Toysmart Database* <http://www.boston.com/dailyglobe2/231/business/Judge_declines_to_rule_on_Toysmart_database+.shtml> (accessed Aug. 21, 2000); *see also* Dow Jones Newswires, *Judge Rejects Toysmart Agreement with FTC* <http://interactive.wsj.com/archive/retrieve/cgi?id=BT-CO-20000817-003698.djml> (accessed Aug. 17, 2000).

British e-tailer sporting the same Web seal, the United Kingdom's Data Protection Law would have required such a result.[123]

The FTC's authority is restricted to a deceptive or unfair practice, which "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[124] This limited grant of power constrains the agency's ability to address privacy issues where there are no promises made, and therefore no deception possible, where no monetary damage is apparent, or where countervailing arguments can be mounted to excuse any breach of fair information practices for commercial expedience.[125] The FTC's mandate, the positions reflected in its reports to Congress, and its recent experiences with self-regulation, highlight a principal feature of the current American policy debate: primacy is given to the fundamental importance of market forces supporting commerce at the expense of other important rights. Consumer safety laws also add to the cost of doing business. Unregulated investment markets can make it easier for some businesses to raise capital. Yet as modern securities and consumer safety commissions teach, confidence in any sector of the economy is not fostered when known and controllable threats to weaker players and honest brokers are left unchecked. Market forces can eventually eliminate the bad actors and reward the good. But much economic and social damage can be done in the meantime. The FTC's role in the American policy debate, while not without value, demonstrates that an oversight agency dedicated to facilitating commerce—and not privacy—as its primary goal, is less well suited than a specialized agency for administering rights to personal data protection. If privacy protection is the objective of privacy law, the traditional U.S. model of FTC oversight, intended to foster desirable commercial and marketplace conditions, should be re-evaluated as an appropriate model for administering U.S. privacy rules.

123. VNUnet.com, *Failed UK Dotcoms Stir up Privacy Storm*, <http://www.vnunet. com/Analysis/1105916> (accessed July 7, 2000). In a similar scenario earlier this year, the receivership of U.K. e-tailer Boo.com, also a recipient of TRUSTe's seal, led to the sale of its database on 350,000 customers to a U.S. company. *Id.* This was in apparent breach not only of its privacy policy, but also of the UK's Data Protection Act, which requires customers to be contacted each time their information is used for another purpose. *Id.* Under U.K. law, customers should have been contacted for their consent in advance of any sale. *Id.* Had the UK's Data Protection Registrar been informed, the sale could have been blocked until this was accomplished. Once the information left the country, there was little that could be done to prevent its use or resale in another country. *Id.*

124. 15 U.S.C. § 45 (n) (1994).

125. *See* Schwartz, *supra* n. 18, at 1609, 1637-1639.

V. INTERNATIONAL IMPERATIVES

The U.S. experience is not inevitable. Robust and effective public and private sector privacy regimes exist in other nations throughout Europe[126] and in Commonwealth countries such as Canada, Australia and New Zealand.[127] In all of these countries, independent Privacy Commissioners have been charged with performing the multiple tasks of oversight, enforcement, research and education, and have engaged in constructive dialogues with governments and the private sector to develop policy options that are protective of individual rights and compatible with national economic interests.

Canada has had a privacy regime with administrative oversight for federal government institutions since the 1970's;[128] and the majority of Canada's provinces also have privacy laws governing public sector institutions within each province.[129] Canada's several privacy commissioners have largely avoided the pitfalls of the U.S. privacy regime by promoting an ethos of personal data protection, and working closely with government to improve practices and ensure compliance.[130] Most recently, Canada's federal Parliament has enacted a new law, which extends similar protections to the federally regulated private sector. The Personal Information Protection and Electronic Documents Act,[131] which takes effect in January 2001, incorporates the full set of fair infor-

126. The European Commission, *Recommendation 1/2000 on the Implementation of Directive 95/46/EC* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp30en.htm> (Feb. 3, 2000) (listing the European nations with existing laws and the status of implementation of the European Directive on the Protection of Personal Data, Directive 95/46/EC of the European Parliament).

127. *Canada's Privacy Act*, R.S.C. 1985, c. P-21 (1985); *Australia's Privacy Act 1988, Information Privacy Principles* § 14 <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Nov. 16, 2000); *New Zealand's Privacy Act 1993, Privacy Amendment Act 1993, Privacy Amendment Act 1994*, <http://www.privacy.org.nz/slegisf.html> (accessed Nov. 16, 2000). *Canada's Personal Information Protection and Electronic Documents Act*, S.C. 2000, C-5 <http://www.privcom.gc.ca/english/02_06_01_01_e.htm> (accessed Nov. 16, 2000).

128. *See Canada's Privacy Act*, R.S.C. 1985, P-21.

129. Information and Privacy Organizations in Canada, <http://www.privcom.gc.ca/english/02_03_01_e.htm> (accessed Aug. 28, 2000).

130. *See e.g.,* Privacy Commissioner, *Annual Report (1999-2000)* <http://www.privcom.gc.ca/english/02_04_08_e.htm> (accessed Nov. 16, 2000); *see also* Information and Privacy Commissioner/Ontario, *Annual Report 1999* <http://www.ipc.on.ca/english/pubpres/ann_reps/ar-99/ar-99e.pdf> (accessed Nov. 16, 2000); The Office of the Information and Privacy Commissioner/British Columbia, *Annual Report 1999-2000* <http://www.oipcbc.org/publications/annual/oipcbc_annual_report_99-2000.pdf> (accessed Nov. 16, 2000).

131. Canada's *Personal Information Protection and Electronic Documents Act*, S.C. 2000, C-5 <http://www.privcom.gc.ca/english/02_06_01_01_e.htm> (accessed Nov. 16, 2000).

mation practices reflected in the OECD Guidelines.[132] Federal oversight authority is given to Canada's existing public sector Privacy Commissioner who can ensure expertise and consistency in its implementation with strong investigative powers and court enforcement mechanisms. Canada's provincial governments have begun to propose their own private sector laws in consultation with consumer and corporate stakeholders and their existing data protection officials.[133] None of these measures are Internet specific, but are intended to apply to both online and off-line activities through technology neutral protections. Canada has also been engaged in dialogue with the European Commission under a work plan designed to ensure the free flow of personal data between the EU and Canada and the continuing development of compatible privacy protection standards in order to facilitate international data transfers.[134]

Of the privacy models that presently exist, the European Directive on the Protection of Personal Data[135] has had the greatest experience with accommodating economic interests and individual rights, as well as the interests of different nations, and is considered by many policy analysts to be the standard by which other national and international initiatives are measured. The Directive starts from the premise that economic prosperity and privacy protections for its citizens are not only compatible, but also complementary. It is expressly designed to promote the economic well-being of the Community's member states and their citizens by facilitating cross-border data flows for economic and social programs and trade expansion, while at the same time respecting the individual's "fundamental rights and freedoms, notably the right to privacy."[136] While all member states are bound by its common principles, the Directive does not seek to impose absolute uniformity on national privacy laws, many of which pre-date it and are derived from their unique legal

132. Canadian Standards Association International, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-95 <http://www.csa.ca/english/home/index.htm (June 3, 2000).

133. *See e.g.*, Ministry of Consumer and Commercial Relations (Ontario), *Consultation Proposal for An Ontario Privacy Act* <http://www.ccr.gov.on.ca/mccr/english/2766_b1a.htm> (accessed Aug. 28, 2000).

134. The European Commission, EU - Canada Summit Lisbon, *Electronic Commerce in the Global Information Society, Work Plan 2000/2001* <http://www.europa.eu.int/comm/external_relations/canada/summit_06_00/elec_com_wk_plan_2000_2001.htm> (June 26, 2000); *see also* The European Commission, *Opinion 1/97 on Canadian Initiatives Relating to Standardization in the Field of Protection of Privacy* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp2en.htm> (May 29, 1997).

135. Directive 95/46/EC, 1995 O.J. (L281/33) ch. 2.

136. *Id.* at Preamble §§1-3.

and constitutional traditions.[137] The Directive also mandates the creation of independent agencies in each state to monitor national laws implementing its provisions and to enforce rules prohibiting the transfer of personal data outside national borders without "adequate levels of protection" in place.[138] Each of these agencies must have investigative powers, effective powers of intervention, powers to engage in legal proceedings, and powers to hear claims concerning the lawfulness of data processing.[139] Existing divergences among national laws have created a great potential for conflicts under the Directive, which in turn has slowed the implementation process. Even among a few member states with strong pre-existing protections, national legislatures have been slow to act and European Union-wide implementation is not yet complete.[140]

---

137. *Id.* at ch. 2, Art. 5. (noting that at the time the EU Directive came into force, there were substantial divergences in the laws of members states, many of which were of long standing). Since 1978, France has had a comprehensive data protection regime, which governs both the public and private sectors, imposes civil and criminal sanctions, and is supervised by a large independent regulatory commission. *Id.* Belgium has a system of more recent vintage (1992) modeled on the French law, and is applicable to computerized and manual data processing, but has no specific rules governing online services. *Id.* Germany was the first nation in the world to enter the privacy arena with the enactment of a data protection law in the state legislature in Hesse in 1970. *Id.* Now all sixteen German states in addition to the federal government have privacy laws with divided and, in some case, overlapping jurisdiction, and varying degrees of oversight. *Id.* In some states private sector oversight is provided through existing data protection commissioners with powers over state agencies, and in other states through separate but still independent supervisory authorities. *Id.* All such agencies had primarily an advisory role, although they could issue directives to correct technical or organizational shortcomings. *Id.* In 1997, the federal Bundestag enacted a comprehensive privacy regime specifically governing online services; this statute relies on existing mechanisms of registration and oversight provided under privacy laws of general application. *Id.*; *see also* Joel R. Reidenberg & Paul M. Schwartz, *Data Protection Law and On-Line Services: Regulatory Responses* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/studies/regul.pdf> (accessed Nov. 16, 2000). By contrast, data protection in the UK was governed by the *Data Protection Act of 1984* which had no specific provisions applicable to the Internet, but which was supervised by a Data Protection Registrar with relatively strong enforcement powers of entry and search pursuant to warrant and authority over registration and de-registration of data processors, the issuance of compliance directives, and the prosecution of offenders. *Id.* National implementing laws have been required to bring consistency to the varying models that existed. *Id.* Varying notice requirements, definitions of personal information, and anonymity requirements have been particularly problematic issues for achieving greater convergence in national treatment under the Directive. *Id.*

138. Directive 95/46/EC, *supra* n. 4, at Art. 25-26, 28.

139. *Id.* at Art. 28(3).

140. The European Commission, *Status of implementation of Directive 95/46* <http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm> (accessed Nov. 16, 2000). The majority of member states have now passed the required national laws, and most others have introduced such measures in their legislatures. *Id.*

The Directive's principal mechanism for overseeing national implementation is the Data Protection "Working Party" comprised of representatives of each nation's independent data protection authorities.[141] By sharing the experience of Europe's oversight agencies, the Working Party has encouraged the adoption of coherent strategies for implementing and applying the Directive's general principles.[142] It has produced evaluations, opinions, guidelines and recommendations on a range of issues, including data protection and the media (dealing with the balance between privacy protection and freedom of the press); the telecommunications industry (recommending that these standards can be transposed to the Internet); e-commerce (for incorporating PET's into electronic payment systems); anonymity on the Internet (the preferred default, subject to law enforcement and authentication needs); notification issues (particularly relating to invisible data collection); data transfers to third countries (assessing when these should be permissible); and self-regulatory codes (which should be complete, binding, verifiable, and enforceable).[143] The Working Party's efforts in evaluating the existing laws, policies and enforcement regimes of member states have added needed support to the implementation process; and its progress reports have brought pressure to bear on recalcitrant members to move their political processes along, under threat of Commission-imposed sanctions.[144]

The European Directive has also brought pressure to bear on the United States to develop "adequate levels of protection" for transfers to U.S. businesses of any personal data originating from within a member state's borders.[145] In March 2000, the U.S. formalized self-regulatory measures for participating American companies, which permitted it to enter into a "safe harbor" accord with the European Commission.[146] Under the terms of the accord, the U.S. Department of Commerce will establish a list of companies that have agreed to adhere to data protection rules providing the adequate level of protection required by the Eu-

141. Directive 95/46/EC, *supra* n. 4, at, Art. 29.

142. The European Commission, *OPINION 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp15en.htm> (accessed Nov. 16, 2000).

143. The European Commission, *Documents adopted by the Data Protection Working Party* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/> (accessed Nov. 16, 2000).

144. The European Commission, *Recommendation 1/2000 on the Implementation of Directive 95/46/EC* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp30en.htm> (Feb. 3, 2000).

145. *Id.*

146. The European Commission, *Opinion 3/2000 on the EU/US Dialogue Concerning the Safe Harbor Arrangement* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp31en.htm> (accessed Nov. 18, 2000).

ropean Directive.[147] Compliance with the rules will be backed by independent dispute resolution mechanisms and, ultimately, by the law enforcement powers of the FTC under section 5 of the FCTA.[148] Companies adhering to the accord may receive transfers of personal data originating within a EU member state without putting the state in breach of the Directive.[149] Data transfers outside the terms of the accord may still be permitted if certain exceptions are satisfied, such as consent, or if alternative safeguards such as contract stipulations are in place.[150] This agreement almost foundered before it was implemented due to the European Parliament's concerns that the U.S. measures lacked sufficient protections in the nature of remedies for aggrieved individuals. The EU Working Party's reports on the negotiations had identified shortcomings in these protections under early proposals and offered constructive suggestions[151] which ultimately permitted the European Commission to ratify the accord in July 2000,[152] thus averting a U.S.-European trade dispute which could seriously have undermined industries dependent on trans-Atlantic data flows.[153] The safe harbor accord has thus accomplished what U.S. legislators have not. It has introduced to American businesses higher privacy standards than those currently

147. U.S. Department of Commerce, *Safe Harbor Privacy Principles* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/shprinciples.pdf> (July 21, 2000).

148. Annex, *List of Statutory Bodies Recognized by the European Union* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/annprinciples.pdf> (accessed Nov. 16, 2000) (noting that the U.S. Department of Transportation exercises regulation over the airline and travel business pursuant to 49 U.S.C. § 51712).

149. *See* Directive 95/46, *supra* n. 4, at Art. 25.

150. *Id.* at Art. 26

151. The European Commission, *Opinion 4/2000 on the level of protection provided by the Safe Harbor Principles* <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32en.htm> (accessed Aug. 28, 2000); *see also* The European Commission, *supra* n. 146.

152. The European Commission, *Data protection: Commission Adopts Decisions Recognizing Adequacy of Regimes in U.S., Switzerland and Hungary* <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm> (July 27, 2000); *see also* The Commission of the European Communities, *Commission Decision of 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* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf> (accessed Nov. 16, 2000).

153. The European Parliament voted earlier in July 2000 to ask the Commission to go back to the bargaining table to secure greater concessions on individual remedies for privacy breaches. The Commission has promised to revisit the accord if Parliament's fears about effective remedies for individuals prove to be well founded. At the same time, the Commission agreed that the data protection laws of Switzerland and Hungary provide adequate protection. Talks with several other countries, including Australia, Canada and Japan are proceeding with a decision on the adequacy of Canada's new privacy laws expected soon.

afforded by domestic U.S. laws and has demonstrated that U.S. priorities can be accommodated within the four corners of a document incorporating fair information practices.

The European case also illustrates that domestic laws alone cannot dictate the pace of progress in establishing online privacy standards. There must be a consensus on the basic objectives of privacy rules and effective means of mediating any differences in priorities and approaches across the full spectrum of stakeholder interests. In order for this process to occur, there must be a forum and incentives for dialogue. The European Directive and its Working Party provide workable models for achieving these objectives. However, Internet privacy regulation ultimately requires global solutions, and no model can work on that scale without a commensurate level of U.S. participation.

VI. MOSAIC OF SOLUTIONS

The greatest challenges to policy makers in the implementation of fair information practices online are those presented by existing divergences in the national treatment of privacy regulation and territorial enforcement issues which cannot be resolved by traditional conflict of laws principles.[154] Some jurisdictions, like Europe, have comprehensive regulatory schemes; others, like the U.S., have narrower legal rules or policies supporting self-regulatory measures; some offer no protections at all. These divergencies can create the potential for disruption in international data flows. Where comprehensive rules already exist among the laws of trading nations, even minor differences in notification requirements or levels of enforcement from nation to nation can produce market distortions and claims of discriminatory treatment under bilateral and multilateral trade agreements.[155]

Complete global harmonization of fixed legal principles for data protection in the context of existing Internet infrastructure design and emerging e-commerce applications is not realistic. On the other hand, the technical architecture and design of the Internet for future applications are important regulatory determinants for the efficacy of online

154. *See* Reidenberg, *supra* n. 18; *see also* Reidenberg & Schwartz, *supra* n. 18, at 144-153; American Bar Association Global Cyberspace Jurisdiction Project, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet* <http://www.kentlaw.edu/cyberlaw/> (accessed Aug. 28, 2000) (providing an exhaustive study of the jurisdictional issues raised in relation to cyberspace); *see generally* Thomas P. Vartanian, *The Confluence of International, Federal, and State Jurisdiction Over E-Commerce: (Part 1),* 2 J. Internet L. 5, (1998); Thomas P. Vartanian, *The Confluence of International, Federal, and State Jurisdiction Over E-Commerce: (Part II),* 2 J. Internet L. 6 (1998).

155. *See* Reidenberg, *supra* n. 18.

data protection.[156] Encryption, anonymizers, and site certification are examples of existing technologies and mechanisms capable of achieving some of these objectives with a measure of flexibility to accommodate varying sectoral or national imperatives. PETs providing users with notice and choice options, like P3P and other intelligent agents for automated information brokering, could potentially accommodate varying regulatory requirements and provide a measure of adaptability to permit the same service provider to offer anonymity or notice choices in certain jurisdictions, or for certain activities, but not others.[157]

Market incentives already exist for industry to develop privacy protective mechanisms,[158] but new incentives must continue to be created for the design of more efficient and transparent technologies. Targeted research and development funding from public and private sector sources can accelerate this process. The procurement decisions of government institutions, with their own data protection responsibilities, can also facilitate an added level of interface between policy development and technology design. National oversight, enforcement and the imposition of liability for egregious violations can ensure that service providers maintain the needed impetus to achieve these same objectives. However, it will only be a "mosaic of solutions" — a mix of regulatory and technology options — that can achieve a comprehensive and balanced approach to online data protection across national borders, accommodating differing legal traditions, regulatory priorities, and enforcement mechanisms.[159]

---

156. *Id.*; *see also* Lawrence Lessig, *Code and Other Laws of Cyberspace*, 163 (Basic Books 1999) (noting Mr. Lessig's argument that in the information age, computer "code" is a fundamental part of the language of law and politics by which we choose to govern or be governed). In cyberspace, and particularly in matters of free speech, privacy and democratic governance, it is up to lawyers, policy makers and citizens to decide on the values that the language of computer technology embodies; Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* 258 (O'Reilly 2000). *Id.* Mr. Garfinkel makes a similar argument to the effect that technology is not neutral, but has design goals, like privacy policy, and that both can be made to coincide. *Id.*

157. *See P3P and Privacy*, *supra* n. 47.

158. Keith Perine Washington, *The Persuader*, The Industry Standard 161 (Nov. 13, 2000).

159. Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* 197-198 (McGraw Hill 1997); *see also* Philip E. Agre, *Technology and Privacy, The New Landscape*, 25 (Philip E. Agre & Marc Rotenberg, eds., MIT Press 1998).

> These technology and policy solutions are potentially complementary; they comprise what Cavoukian and Tapscott have called a 'mosaic of solution.' It will require great effort to determine the appropriate combination of means to protect privacy in particular settings. PETs in particular must travel a long road from theory to practice, and it will be important to document and analyze their first application. The new technologies' great promise will also require theoretical innovation. As relationships are mediated by technology in more sophisticated ways, designers and policy makers will need more complex theories of agency and

A number of organizations now exist for engaging in international cooperation and mediating these divergences on a global scale. The OECD has recently been active in re-examining these issues from an economic development perspective at a December 1998 Ottawa summit and in other venues.[160] The World Trade Organization ("WTO") has assumed a limited but significant role under trade accords, which restrict prohibitions on trans-border data flows.[161] While these accords make exceptions for personal data transfers, they are subject to claims of discriminatory treatment and challenges to the legitimacy of any exceptions claimed. The World Intellectual Property Organization is active in the area of data ownership, electronic rights management, and the adaptation of intellectual property rights to electronic commerce.[162] All of these efforts can have an impact on the framework within which online privacy issues are resolved on an international scale. Proposals have also been made for a new international trade accord in the nature of a "General Agreement on Information Privacy" (GAIP), which would operate at a

---

trust in technological environments. Perhaps most important, future research should clarify the relationship among technology, privacy and association.

Id.

160. Organisation for Economic Co-operation and Development, *Privacy Protection in a Global Networked Society: An OECD International Workshop with the Support of the Business and Industry Advisory Committee (BIAC) Paris*, DSTI/ICCP/REG(98)5/FINAL, 9 (Feb. 16-17, 1998). In February 1998, the OECD sponsored the International Workshop on Privacy Protection in a Global Networked Society workshop in Paris. *Id.* Representatives from a number of the European Data Protection Commissioners' offices participated. *Id.* The workshop's "objective was . . . to bring together representatives from the 29 OECD Member countries to engage in a dialogue among governments, the private sector, the user and consumer communities, and data protection authorities to focus on how the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* may be implemented in the context of global networks." *Id.*; *see also* Organisation for Economic Co-operation and Development, *Consumer Protection in the Electronic Marketplace* DSTI/CP(98)13/REV2, 5 (Oct. 8-9, 1998) (noting that in October 1998, the OECD held its Ministerial Conference in Ottawa called *A Borderless World: Realising the Potential of Global Electronic Commerce*); Anne Carblanc, *Data Protection on Global Networks in the Context of Electronic Commerce — Recent Activities of the OECD*, Datenschutz — Brücke zwischen Privatheit und Weltmarkt Symposium <http://www.datenschutz-berlin.de/informat.heft27/carblanc.html> (Dec. 23, 2000). The OECD is now preparing a report on the use of contractual solutions for transborder data flows. *Id.* The report will examine, in the context of business-to-business as well as consumer-to-business contracts, issues such as content of contracts, certification and labeling and rights of data subjects; the report also will examine dispute resolution mechanisms and enforcement, such as mediation, arbitration, litigation, and remedies. *Id.*

161. Int'l News, *Electronic Commerce: Electronic Commerce Under Services Agreement, WTO Report Says*, BNA Banking Rpt. (July 27, 1998).

162. Joel Reidenberg, Symposium, *Cyberspace and Privacy: A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules In Cyberspace*, 52 Stan. L. Rev. 1315, 1354 (2000).

government to government level of negotiation.[163]

Of all the mechanisms presently available for addressing Internet privacy issues and achieving international convergence in online data protection rules, the world's ever-growing number of data protection authorities offers the greatest promise. Privacy Commissioners have extensive experience with administering fair information practices under national laws, are institutionally imbued with the ethos of personal privacy protection, understand its technological implications, and are sensitive to inter-jurisdictional differences.[164] Individually and collectively, they serve as international emissaries of data protection principles and the rights of individuals.[165] Through working groups, annual conferences, special symposia and ad hoc contacts, they have forged partnerships with their colleagues in all nations where they presently exist,[166]

---

163. *See* Reidenberg, *supra* n. 18.

164. David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective*, in *Technology and Privacy, The New Landscape, Introduction* 167 (Philip E. Agre & Marc Rotenberg, eds., MIT Press 1998). David Flaherty, Former Information and Privacy Commissioner of British Columbia, describes the multiple roles played by privacy commissioners and the range of influence they can have on public policy development, not just the enforcement of existing privacy laws. *Id.*

165. *See* Reidenberg, *supra* n. 18.

166. Privacy Commissioner's Office, *21st International Conference on Privacy and Personal Data Protection* <www.pco.org.hk/conproceed.html> (Sept. 13, 1999); *see also* Lorrie Faith Cranor, *Agents of Choice: Tools That Facilitate Notice and Choice About Web Site Data Practices* <www.pco.org.hk/conproceed.html> (Sept. 13, 1999); Austin Hill, *The Privacy Risks of Public Key Infrastructures* <www.pco.org.hk/conproceed.html> (Sept. 13, 1999); David Banisar, *Privacy and Data Protection Around the World* <www.pco.org.hk/conproceed.html> (Sept. 13, 1999); Alfred Bullesbach, *Data Protection and Privacy at a Global Enterprise* <www.pco.org.hk/conproceed.html> (Sept. 13, 1999); Italian Data Protection Commission, *Towards An Electronic Citizenship* <www.garanteprivacy.it/garante/frontdoor/1,1003.00.html?LANG=2> (Sept. 28-30, 2000); Ann Cavoukian, *Should the OECD Guidelines Apply to Personal Data Online?* (publication forthcoming 2000); Office of the Information and Privacy Commissioner/Ontario Best Practices for Online Privacy Protection, Exhibit B in Information and Privacy Commissioner/Ontario, A Report to the 22nd International Conference of Data Protection Commissioners (Venice, Italy), *Should the OECD Guidelines Apply to Personal Data Online?* (publication forthcoming 2000); Information and Privacy Commissioner/Ontario Canada & Registratiekamer The Netherlands *Privacy-Enhancing Technologies: The Path to Anonymity (Volume I)* <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/anon-e.htm> (accessed Nov. 16, 2000); Descriptions of Papers, *Privacy-Enhancing Technologies: The Path to Anonymity (Volume II)* <http://www.ipc.on.ca/english/pubpres/sum_pap/summary.htm> (Aug. 1995); Independent Centre for Privacy Protection Schleswig-Holstein, Germany, *The Virtual Privacy Office and Its Modules* <http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/projekte/virdsb/module_e.htm#1> (June 22, 2000) (noting that the Privacy Commissioner of Schleswig-Holstein has initiated the "Virtual Privacy Office," a joint venture of privacy protection authorities created with a view to facilitating international cooperation for global privacy and is open to all privacy protection authorities); Bruno Baeriswyl, Helmut Bäumler, John J. Borking, & Marit Köhntopp, The *Virtual Privacy Office — A New Approach to Privacy Protection* <http://www.koehntopp.de/marit/publikationen/privacyoffice/BBBK_Submission_to_ISSE_

as well as important relationships with domestic and foreign governments, and industry and technology standards associations, as advisors and consultants on a broad range of policy fronts.[167] Their contribution should be expanded and formalized.[168] It has been put forward that data protection officials "must have political input into the technical infrastructure decisions that affect the nature and characteristic of data flows and do so through a broader range of regulatory policy instruments, such as the standardization of technology specifications and the redesign of infrastructures, rather than the traditional legal directive approach."[169] The European Union's Working Party has demonstrated that much can be accomplished by the collective efforts of national privacy commissioners working within a framework of international cooperation. A broader framework for a General Agreement on Information Privacy is one mechanism for accomplishing these objectives beyond Europe's borders; other options should also be explored.

VII. A REASON FOR CHANGE

At the same time we must not forget why these issues should concern us. Privacy is not simply a commercial inducement to engage in business on the Internet — it is a fundamental human right.[170] History has

---

2000.pdf> (June 22, 2000) (noting that presently, the Federal Commissioner for Data Protection, Germany, the Data Protection Commission, Netherlands, and the Privacy Commissioners in Switzerland, as well as a number of regional European offices for privacy protection have expressed their intention to cooperate in the project, with Ontario recently joining the project).

167. Office Of Justice Programs Integrated Justice Information Technology Initiative, *Privacy Design Principles for an Integrated Justice System: Working Paper* <www.ojp.usdoj.gov/integratedjustice/pdpapril.htm> (accessed Sept. 8, 2000) (noting that the staff at the Information and Privacy Commissioner/Ontario are assisting Ontario's Integrated Justice initiative in its privacy impact assessment and are working on various privacy-related matters). The Information and Privacy Commissioner/Ontario has been collaborating with the United States Department of Justice, Office of Justice Programs and others in developing two papers addressing privacy design principles and a privacy impact assessment for Integrated Justice. *Id.*; *see also* Office of Justice Programs Integrated Justice Information Technology Initiative, *Privacy Impact Assessment for Justice Information Systems: Working Paper* <www.ojp.usdoj.gov/integrated justice/piajis.htm> (accessed Sept. 8, 2000); *P3P and Privacy*, *supra* n. 47. (noting that the Information and Privacy Commissioner/Ontario has been having discussions with the Ontario government regarding its public key infrastructure (PKI) initiatives and has offered comment on its various design model options and the staff at the Information and Privacy Commissioner/Ontario are consulting with W3C on the P3P program)

168. Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* 260-62 (O'Reilly 2000).

169. Reidenberg & Schwartz, *supra* n. 18, at 148, 152-53.

170. Privacy International, *Privacy & Human Rights 1999* <http://www.privacy international.org/survey/summary.html> (accessed Oct. 24, 2000). The Privacy Report indicates that privacy is a fundamental right recognized by all major international treaties and

taught the hard lesson that incursions on individual rights of dignity and privacy can have a profound impacts on political and social structures. When those incursions affect virtually all aspects of life in an increasingly wired world, the potential for fostering undesirable social and political conditions is magnified enormously. It may be considered trite that personal privacy is intimately associated with basic values of human dignity and personal autonomy: it has been termed "the fundamental right from which all others are derived."[171] It is sometimes less apparent that individual privacy is also essential to our basic political and economic freedoms and the institutional choices we make as a society: its absence, among other things, risks "chilling the freedom of association on which any possibility of democratic community is based."[172]

If the totality of every person's online experience is captured, warehoused, profiled and data-mined with ever-increasing sophistication and accuracy, human behavior can be adversely and ineluctably altered on an individual and societal basis. Individuals cannot express an online thought or interest without permanently being associated with it, and having it linked not only with their other thoughts and interests, but with those of other individuals who have visited the same sites, made similar searches or inquiries, or expressed similar views on a particular topic. Individual habits are tracked in time, space, frequency, and priority though a myriad array of clickstream data. A mouse click on an icon or banner ad reveals susceptibility to particular messaging or imagery. Individuals are manipulated according to a set of rules or code that lurks somewhere behind their computer screens, and of which they are only vaguely aware. Their online choices are recorded, analyzed, and expanded or contracted, their attitudes imperceptibly altered, by their virtual experiences. They may or may not choose to use the Internet as a tool for learning about a spouse's treatable illness or what really happened at Waco, or simply to manage their investment portfolios, political affiliations, shopping needs, or plans to travel abroad, for fear that a business competitor, bank, medical facility, insurance company, employer or government agency may gain access to their online personality and use it, unbeknownst to them, to affect adversely some entitlement or privi-

---

agreements on human rights. *Id.* It provides that there is, at a minimum, an implicit right to privacy in numerous international documents involving human rights. *Id.*; *see also United Nations Declaration of Human Rights,* G.A. res. 217(a) (III), (1948), U.N. Doc A/810 at 71. "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation." *Id.* "Everyone has the right to the protection of the law against such interference or attacks." *Id.*

171. *See* Garfinkel, *supra* n. 168, at 257-58.

172. *See* Agre, *supra* n. 159, at 7-8, 26. Agre makes the point that the "digital persona" described by some authors as increasingly central to the construction of an individual's social identity is also important to the means by which we are governed and to the social, political and economic choices we make. *Id.*

lege. What is worse, the vast majority of North American Internet users is already profiled in this fashion, with no effective recourse to control the data already there, or the even greater incursions upon their digital selves that time and technology will inevitably bring. The value of the Internet as a beneficial tool for education, commerce, democratic governance, and the advancement of individual freedom, is inestimably diminished in the absence of an effective and enforceable regime for personal data protection.

VIII. CONCLUSIONS — THE CASE FOR A U.S. PRIVACY COMMISSIONER

Voluntary self-regulation and marketplace incentives alone cannot ensure that online privacy rights will be adequately protected. The Federal Trade Commission, with a complaint-driven mandate over commercial activities and unfair business practices, is not up to the task: it does not bring to the table the ethos and expertise in fair information practices necessary to ensure appropriate and consistent levels of oversight. What has been missing from the American experience is a comprehensive data protection law with an independent and specialized oversight body to grapple with the difficult issues facing America and other nations today. Options presented in the 106th Congress for immediate solutions to Internet privacy regulation are appealing, but the traditional FTC oversight model is not. A Privacy Commission charged with the task of reviewing data protection issues in the online and off-line worlds, and in both the public and private sectors, on the other hand, can start to level the regulatory playing field and open up a door for the creation of a permanent agency capable of entering into constructive dialogue for global action.

International treaty obligations, enshrined in national privacy statutes overseen by local privacy commissioners, can achieve a measure of rationality in the implementation of privacy rules and in the development of policies and technological standards by which their requirements can be met. As a leader in global trade, information technology, and human rights issues, the U.S. requires no less a privacy protection regime and no less an oversight agency to administer the regime to contribute to the formulation of international solutions. Without American participation at this level, privacy rights on the Internet will remain exposed in the U.S., and in turn, in the global forum.