Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?

Jonathan P. Cody

Follow this and additional works at: https://scholarship.law.edu/lawreview

Recommended Citation

This Comments is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Law Review by an authorized editor of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.
COMMENTS

PROTECTING PRIVACY OVER THE INTERNET: HAS THE TIME COME TO ABANDON SELF-REGULATION?

Jonathan P. Cody

"You already have zero privacy. Get over it."
—Statement of Scott McNealy, Chief Executive Officer, Sun Microsystems, Inc.

With an estimated 171 million users worldwide,² the Internet³ is rapidly changing the way people communicate, purchase goods and services, and transact business.¹ What began as a computer network developed for the Department of Defense three decades ago is today the driving force behind a new global information-based economy.⁵ Although the Internet is

¹J.D. Candidate, May 2000, The Catholic University of America, Columbus School of Law

²See Nua Internet Surveys, How Many Online? (visited June 15, 1999) <http://www.nua.ie/surveys/how_many_online/index.html> (providing an "educated guess" of 171.25 million worldwide users online as of May 1999). The breakdown of users by geographical area is as follows: United States/Canada, 97.03 million; Europe, 40.09 million; Asia and Pacific Island nations, 26.97 million; Latin America, 5.29 million; Africa, 1.14 million; and the Middle East, 0.88 million. See id.

³See HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY: PRIVACY • ACCESS • INTELLECTUAL PROPERTY • COMMERCE • LIABILITY 5 (1996) (defining the Internet as "an international network of computers and computer networks connected to each other").


⁵See Robert D. Hof et al., The "Click Here" Economy, BUS. WK., June 22, 1998, at 122, 122 (arguing that the Internet will create a new economy "that will leave no business or industry untouched"). The Department of Commerce argues that growth in the num-

1183
undergoing exponential user growth, individuals cite concerns about privacy as the primary reason for not using the Internet.  

Fueling online individual privacy concerns is the fact that the collection and use of personal identifiable information have never been cheaper or easier than in the online environment. Such information can be obtained from users and commercial transactions on the Internet will lead to growth in all sectors of the economy. See U.S. DEP’T OF COMMERCE, THE EMERGING DIGITAL ECONOMY 7 (1998) [hereinafter DOC ECONOMY REPORT], available at <http://www.doc.gov/economy/viewhtml.htm>. The commercial transactions that take place over the Internet, either business-to-business or business-to-consumer, are known as “electronic commerce.” See BILL GATES WITH COLLINS HEMINGWAY, BUSINESS @ THE SPEED OF THOUGHT: USING A DIGITAL NERVOUS SYSTEM 443 (1999). The Department of Commerce estimates that commerce over the Internet between businesses alone will reach $300 billion annually by the year 2002. See DOC ECONOMY REPORT, supra, at 7, 13.

The Internet was created in 1969 for the Department of Defense to serve as a national communications network that could afford continuous communications capabilities even if some of the network had been damaged in a time of war. See Reno v. ACLU, 521 U.S. 844, 849-50 (1997) (discussing the birth and history of the Internet). For a discussion of the origins and technological history of the Internet from some of its creators, Barry M. Leiner et al., A BRIEF HISTORY OF THE INTERNET (last modified Feb. 20, 1998) <http://www.isoc.org/internet/history/brief.html>.

6. See Business Week/Harris Poll: Online Insecurity, BUS. WK., Mar. 16, 1998, at 102, 102 [hereinafter Business Week Poll]. A Business Week/Harris poll found that 61% of those surveyed who are not online would be more likely to start using the Internet if their privacy were protected online. See id. Seventy-eight percent of those polled who are already online would use the Internet more if their privacy were protected. See BW/Harris Poll: Online Insecurity (last modified Mar. 5, 1998) <http://www.businessweek.com/1998/11/b3569107.htm> [hereinafter Business Week Poll-Web]. The full results of the Business Week/Harris poll can be found at Business Week’s Web site. See Business Week Poll supra, at 102.

7. For the purpose of this Comment, “personal identifiable information” is defined as any information that can be traced to a particular Internet user or to that user’s computer. This Comment does not consider, however, the protection of children’s personal identifiable information online. Congress enacted the Children’s Online Privacy Protection Act of 1998 (COPPA) to regulate the collection and use of personal identifiable information from children under the age of 13 on the Internet. See Children’s Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (Supp. III 1997); 15 U.S.C. § 6501(1) (defining the term “child” as an individual under the age of 13).

The COPPA requires a Web site, online service, or operator that knowingly collects a child’s personal identifiable information, to provide notice as to what information they collect, how the information is used, and the entity’s disclosure practices. See 15 U.S.C. § 6502(b)(1)(A)(i) (Supp. III 1997) (requiring the Federal Trade Commission to promulgate regulations to implement this mandate). A Web site, online service, or operator must “also obtain verifiable parental consent for the collection, use or disclosure of personal information from children.” 15 U.S.C. § 6502(b)(1)(A)(ii). The COPPA provides for exceptions to the parental consent mandate, and safe harbor provisions for companies. See 15 U.S.C. § 6502(b)(2)(A)-(E) (governing the situations where “verifiable parental consent” is not required); 15 U.S.C. § 6503 (stating that companies may satisfy the COPPA by following a set of approved industry issued self-regulatory guidelines).

8. See FEDERAL TRADE COMM’N, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS 3-4 (1997) [hereinafter FTC IRS REPORT] (discussing the technological
tained from an online user in a variety of ways, with or without the user’s knowledge. For example, through the use of a “cookie,” or by tracking a user’s “clickstream,” a Web site (or “site”) can determine a user’s electronic mail address, the type of computer he is using, what information the user accesses on the Web site, and how long the user visits the site, all without the user’s consent.

Developments that have led to cheaper and easier ways to collect detailed personal identifiable information, available at <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm>; Bureau of Consumer Protection, Federal Trade Comm’n, Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure 1 (1996) [hereinafter FTC Staff Report] (stating that the Internet allows for a less expensive means “to gather, store, analyze, transmit, and reuse” personal identifiable information that was “unimaginable just a few years ago”), available at <http://www.ftc.gov/reports/privacy/privacy1.htm>.

9. See Federal Trade Comm’n, Privacy Online: A Report to Congress 3 (1998) [hereinafter FTC Privacy Report] (explaining the variety of means employed by commercial Web sites to collect personal identifiable information from online users), available at <http://www.ftc.gov/reports/privacy3/toc.htm>; FTC Staff Report, supra note 8, at 4-5 (commenting that personal identifiable information gathering can take place either with the user’s consent or without his knowledge).

10. See Joshua B. Sessler, Note, Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet, 5 J.L. & Pol’y 627, 632-34 (1997) (describing the cookie and its functions). A cookie is a user file that is attached to an online user’s hard drive when he visits a Web site. See id. at 632. The cookie allows the Web site to save certain user information, such as a password, so the site may identify that particular user and his preferences each time the user visits that site. See id. at 632-33.

11. See FTC Staff Report, supra note 8, at 3-4 (describing a clickstream as a user’s path through the Internet, which can be tracked, stored, reused, and aggregated).

12. See id. (explaining that a Web site can track both information about a visitor as he enters the site and the visitor’s “browsing activities” while visiting the site); see also Susan E. Gindin, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 San Diego L. Rev. 1153, 1170 (1997) (stating that Web sites, by using cookies, can track a visitor’s computer type, the software the visitor is using, the amount of time the visitor spends on each page of the Web site, and the Web site from which the visitor linked). In fact, unique identifying serial numbers that are contained in products produced by Microsoft Corporation and Intel Corporation can be used to track individual computer users. See Peter H. Lewis, You Say You Want Evolution?, N.Y. Times, Mar. 4, 1999, at E1 (explaining that the Intel chip’s “Processor Serial Number” can follow individuals on the Internet by tracking their computers when users are online, even if the user has disabled the feature); John Markoff, Growing Compatibility Issue: Computers and User Privacy, N.Y. Times, Mar. 3, 1999, at A1 (noting that identifying serial numbers can be found in Microsoft’s Windows 95 and Windows 98 operating systems and its Word and Excel programs, and in Intel’s recently released Pentium III microprocessing chip); John Markoff, Microsoft to Alter Its Software, Responding to Privacy Concerns, N.Y. Times, Mar. 7, 1999, § 1, at 1 [hereinafter Markoff, Microsoft] (stating that the identifiable number contained in the Microsoft products “could result in the ability to track a single user and the documents he created across vast computer networks”). Privacy advocates fear that such numbers will allow for the misuse of personal identifiable information, while the companies argue the numbers are essential to protect the security and efficiency of the network. See id. (citing the creation of electronic monitoring systems and the tracking of a user’s path through the Internet, and the creation of personalized files on computer users.
A Web site also can collect personal identifiable information by obtaining it voluntarily from the user. For instance, such information can be obtained directly from the online user through online contests, surveys, the purchase of goods or services online, or registration to use a site. Aware that a particular Web site is collecting personal identifiable information, however, many users either are not providing the information and leaving the site or they are providing false information in order to obtain the benefits of the site while keeping their true personal identifiable information private.

Notwithstanding Internet users' concerns about privacy, the collection of personal identifiable information can provide many economic benefits to both businesses and consumers. There are several profitable industries in the business of collecting and using online users' personal identifiable information as concerns among privacy advocates; and stating Microsoft's position that the number would allow support personnel to “help users diagnose problems with their computers more accurately”); see also Lewis, supra, at E1 (explaining that Intel asserts that the serial number is a security feature that enables network employees to prevent against unauthorized use of the network and to diminish fraudulent electronic commerce transactions).

13. See FTC PRIVACY REPORT, supra note 9, at 3 (listing the various means of collecting information directly from an online user by a commercial Web site).

14. See id.; see also Electronic Privacy Information Center, Surfer Beware: Personal Privacy and the Internet (visited Mar. 11, 1999) <http://www.epic.org/reports/surfer-beware.html> (finding, in a June 1997 survey, that 49 out of the top 100 visited Web sites collect personal identifiable information “through on-line registrations, mailing lists, surveys, user profiles, and order fulfillment requirements”).

15. See The Center for Democracy and Tech., Survey Questions (visited Apr. 2, 1999) <http://www.cdt.org/privacy/survey/findings/results.html> [hereinafter CDT Survey] (concluding that “an overwhelming majority of users avoid registering at web sites and giving out personal information online” in order to protect their privacy). A survey conducted by the Center for Democracy and Technology found that nearly 87% of those polled do not provide information when asked and 36% provide false information. See id. at question 1 (hyperlink) (asking respondents if they avoid engaging in the listed activities on the Internet due to concerns about privacy); see id. at question 6 (hyperlink) (asking “[w]hat steps are you taking to protect your privacy online”); see also Business Week Poll-Web, supra note 6 (finding that 59% of those polled never provide information when a Web site requests that the individual register with the site by providing personal identifiable information before gaining access to the content of the site).

16. See FTC STAFF REPORT, supra note 8, at 1 (citing more efficient commerce and lower advertising costs as benefits that the free flow of information brings to the business community, while consumers gain the ability to access more information in less time); Denise Caruso, Digital Commerce: Personal Information Is Like Gold in the Internet Economy, and the Rush Is on to Both Exploit It and Protect It, N.Y. TIMES, Mar. 1, 1999, at C4 (noting that people and companies “are rushing to cash in on the data gold rush” that the Internet produces). “[E]very customer action on a Web site, from a simple click-through to a complex buying transaction or product configuration, generates data that can be captured and mined. . . . Savvy companies aren't just dealing with this flood of data, they're embracing it.” Clinton Wilder, Tapping the Pipeline, INFO. WK., Mar. 15, 1999, at 38, 38.
By tracking an individual's preferences online, companies can use the Internet to produce more efficient and targeted advertising to meet that individual's needs, thus presenting the individual with products he likely will desire. Tailored advertising can be vital to the growth of electronic commerce because, as marketing costs fall, more companies will begin to conduct more commerce over the Internet, which in turn will lead to lower overall prices for consumers around the world.

The tracking of user information on the Internet to provide tailored advertisements originally was done by individual companies; however, with the growth of users on the Internet, and in turn the growth of indi-
individual data derived from the Internet, companies now are turning to third parties to store and analyze this information to create individual user profiles. 21 Many online users believe, however, that the concomitant loss of privacy outweighs the benefits that may arise from tailored advertising or third party use of their personal identifiable information. 22 From this situation, two interrelated questions emerge: (1) how can a balance be struck between the economic benefits of the collection and use of personal information, and the privacy interests of online users; and (2) who should be responsible for striking this balance?

In the United States, the Clinton administration answered the “who” question by supporting private sector efforts to protect the privacy of online users’ personal identifiable information through “self-regulatory privacy regimes.” 23 On July 1, 1997, President Clinton addressed the

21. See Wilder, supra note 16, at 40 (citing difficulties in analyzing information generated by the Internet as one reason companies hire third parties to “help put it to marketing and business use”); see also Teresa Riordan, Patents: Combing the Web for Data on Consumers That Will Let Companies Aim Ads More Effectively, N.Y. TIMES, Dec. 7, 1998, at C9 (noting that companies are tracking Internet user behavior, storing that information, and then developing profiles of the consumers). Software applications known as “data mining” allow Web sites and online marketers to track consumers browsing and buying activities on the Internet. See Baig et al., supra note 1, at 86-87 (explaining that the technologies that banks and telecommunications companies have used for years to track consumer trends are now becoming available for the Internet). The technology provides companies with a means to combine information gathered from different Web sites to produce user profiles. See Riordan, supra, at C9 (stating that a company called Be Free, Inc., which has a patented system to compile information from different Web sites into a vast database, has 20 million individual Internet user profiles collected over only 13 months; and that Engage Technologies currently has a database of 30 million unique user profiles). “With data-mining software, ‘people can be segmented any way a company wants to slice and dice them.’” Baig et al., supra note 1, at 88. Not only are companies employing third parties to analyze data, but companies operating Web sites that collect personal identifiable information often sell this data to third parties. See id. at 86 (stating that companies may sell information that a visitor to their site is willing to provide without the visitor’s knowledge).

22. See Baig et al., supra note 1, at 87 (stating that a Business Week/Harris poll conducted in March 1999 found “that two-thirds of American adults are ‘not willing at all’ to share personal and financial information about themselves online in return for more targeted advertising”); Business Week Poll-Web, supra note 6 (finding that 62% of Internet users are not willing to share personal identifiable information so that companies can provide targeted online ads); CDT Survey, supra note 15, at question 10 (hyperlink) (finding that the most pressing privacy issue on the Internet is the sale of personal information).

23. See FRAMEWORK, supra note 4, at 18 (noting that the Clinton administration’s policy is to prefer industry self-regulation over government intervention at this point in the development of electronic commerce); Edmund L. Andrews, European Law Aims to Protect Privacy of Data, N.Y. TIMES, Oct. 26, 1998, at A1 (noting that the American policy is one under which various industries would police themselves through a self-regulatory regime). Self-regulation is defined as a “process by which norms are set by industry code or corporate direction rather than by legislation or regulation.” Martin E. Abrams, Ex-
"how" question when he directed
the Secretary of Commerce and the Director of the Office of
Management and Budget to encourage private industry and
privacy advocacy groups to develop and adopt within the next
12 months effective codes of conduct, industry developed rules,
and technological solutions to protect privacy on the Internet
consistent with the Privacy Principles issued by the Information

The Clinton administration believes that self-regulation, rather than
government interference, can protect individual privacy while maintain-
ing the free flow of information that is vital to the twenty-first century in-
formation economy.25

Recognizing that the Internet is global in nature, the United States has
participated in discussions among members of the Organisation for Eco-
nomic Co-operation and Development (OECD) to examine ways to im-
plement privacy principles on international networks to protect individu-
als and to facilitate consumer confidence in electronic commerce.26 In

perian's Values Approach to Privacy, in PRIVACY AND SELF-REGULATION IN THE
INFORMATION AGE 259, 259 (U.S. Dep't Commerce, 1997).

24. Memorandum on Electronic Commerce, 33 WEEKLY COMP. PRES. DOC. 1006,
1009 (July 1, 1997) [hereinafter President's Directive], available in 1997 WL 367091. The
White House formed the Information Infrastructure Task Force (IITF) to develop and
implement policies regarding the Internet. See IITF, About the President's Information
Infrastructure Task Force (visited May 17, 1999) <http://www.iitf.nist.gov/about.html>; see
also infra notes 125, 143-154 and accompanying text (describing the IITF's role in U.S. on-
line privacy policy).

25. See FRAMEWORK, supra note 4, at 16-19 (articulating a policy favoring self-
regulatory regimes to balance these conflicting interests). The Clinton administration
thinks that undue regulation of the Internet will hinder the online marketplace's develop-
ment, and also believes that due to the fact that the private sector financed much of the
Internet's expansion, they should continue to lead. See id. at 4 (arguing that unnecessary
regulation will cause a decrease in supply and a corresponding increase in consumer costs
of goods and services offered online).

26. See generally ORGANISATION FOR ECON. CO-OPERATION AND DEV., OECD
MINISTERIAL CONFERENCE "A BORDERLESS WORLD: REALISING THE POTENTIAL OF
GLOBAL ELECTRONIC COMMERCE": CONFERENCE CONCLUSIONS, Doc. No.
SG/EC(98)14/REV6 (1998) [hereinafter OECD E-COMMERCE CONCLUSIONS] (discuss-
ing conclusions reached at an October 1998 OECD conference in Ottawa, Canada, re-
arding privacy and electronic commerce, in which the United States took part), available at
<http://www.ottawaeoeconference.org/english/information/outcomes.html> (hyper-
link—"Conference Conclusions"); ORGANISATION FOR ECON. CO-OPERATION AND
DEV., PRIVACY PROTECTION IN A GLOBAL NETWORKED SOCIETY: AN OECD
INTERNATIONAL WORKSHOP WITH THE SUPPORT OF THE BUSINESS AND INDUSTRY
ADVISORY COMMITTEE (BIAC), Doc. No. DSTI/ICCP/REG(98)5/FINAL (1998) [here-
inafter OECD PARIS PRIVACY REPORT] (describing a workshop that presented issues on
the protection of privacy and the free flow of personal data over the Internet), available at
<http://www.oecd.org//dsti/sti/secur/act/privnote.htm> (hyperlink). The OECD is an
international organization, consisting of 29 member countries, that "provides governments
1980, the OECD released its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* to serve as a set of fair information practice principles that companies throughout the world should recognize in the collection and use of personal identifiable information. In 1998, in light of the rapid development of the Internet and the growth of electronic commerce throughout the world, the OECD examined if, and how, these principles can be applied to the online world. In doing so, the OECD approached the "who" question by recognizing that some countries prefer industry self-regulation, while other countries prefer that their governments play a more active role in protecting their citizens' privacy over the Internet.

While the United States has been hesitant to regulate the Internet, primarily because its growth has been a result of private sector investment, other countries have passed or are considering legislation to protect individual privacy over the Internet. In October 1998, the European Union’s (EU) Data Privacy Directive (the "Directive") came into force, harmonizing the data protection laws of the fifteen EU members. The Directive sets forth general principles for the protection of individual privacy rights in the processing of personal data and for the free flow of allowable personal data.

---


29. See id. at 9 (noting that 34 countries have adopted data protection legislation and those countries that do not rely on legislation tend to apply industry-wide standards).

30. See supra note 25 and accompanying text (discussing the Clinton administration's policy for the private sector to continue the lead in developing the Internet); see also infra Parts II.B-C (discussing the European Union and Canadian approaches to protecting privacy online).


32. See id. at 39-45 (describing the "general rules on the lawfulness of the processing of personal data").
Canada, like the United States, has attempted to protect the personal identifiable information of its citizens through industry self-regulation. Unlike the United States, however, Canada has established a voluntary national standard for the collection and use of personal identifiable information. Currently, Canada is attempting to protect its citizens' personal identifiable information further by codifying privacy protection principles that would apply to the Internet.

The actions taken by both the EU and Canada, as well as the passing of President Clinton's July 1, 1998 deadline for the establishment of an effective self-regulatory regime to protect privacy, present a timely opportunity to assess whether self-regulation in the United States is truly the most effective means to protect the privacy interests of individuals online. This Comment studies the current state of regulation, or lack thereof, concerning privacy of personal identifiable information on the Internet and examines the regulatory structures for online privacy currently in place in the United States, the EU, and Canada. Part I explores the development of a privacy right in the United States through judicial decisions and legislative action. Part II provides an overview of the development of self-regulation to protect privacy online in the United States, the regulatory means of protecting online privacy in the EU and Canada, and actual industry practices used in the implementation of a self-regulatory regime to protect the privacy of individuals on the Internet. Part III analyzes the pitfalls of the current self-regulatory regime. Part IV suggests that the United States Government take action to pro-


35. See Bill C-54, Personal Information Protection and Electronic Documents Act, 1st Sess., 36th Parl., 1996 [hereinafter Bill C-54] (proposing "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed"), available at <http://www.parl.gc.ca/36/1/parlib/chambus/house/bills/government/C-54/C54_2/90052be.html>.

36. See President's Directive, supra note 24, at 1009 (directing the Commerce Secretary and Director of the Office of Management and Budget to assist private industry to develop a self-regulatory regime within 12 months of the release date of the Directive); see also supra text accompanying note 24 (quoting the President's Directive).
tect online users' privacy of personal identifiable information. This suggestion includes formal adoption of fair information privacy practice principles, as well as the creation of a new privacy regulatory authority to ensure that self-regulatory efforts do not fall by the wayside.

I. PRIVACY IN THE UNITED STATES

The idea of a right to privacy in the United States first emerged when Samuel Warren and Louis Brandeis wrote an article introducing the concept of a "right 'to be let alone'" in the late 1800s. In the 100 years since the Warren and Brandeis article, the judicial and legislative branches of the government have granted privacy rights on a sectoral basis.

The Supreme Court has inferred an individual privacy right from the Constitution's Bill of Rights for certain personal decisions and situations. In addition, Congress, through piecemeal legislation, has extended these privacy rights with respect to the collection, use, and distribution of personal identifiable information by the government and private entities.

37. See Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 195 (1890). The "right 'to be let alone'" described by Warren and Brandeis developed into what is now known as tort law privacy. See Ken Gormley, One Hundred Years of Privacy, 1992 WIS. L. REV. 1335, 1345 (noting that the right to privacy expressed by Warren and Brandeis amounted to a basic tort action); Warren & Brandeis, supra, at 219 (stating that a violation of the right to privacy would produce "[a]n action of tort for damages in all cases").


39. See Paul v. Davis, 424 U.S. 693, 713 (1976) (labeling decisions "relating to marriage, procreation, contraception, family relationships, and child rearing and education" as those that are protected under an individual right to privacy); Roe v. Wade, 410 U.S. 113, 153 (1973) (stating that the right to privacy implicit in the Constitution is broad enough to include a woman's decision to terminate her pregnancy); Loving v. Virginia, 388 U.S. 1, 12 (1967) (holding that the government cannot intrude upon an individual's right to marry); Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (holding that a Connecticut law condemning the use of contraceptives violated the right of marital privacy).

40. See Griswold, 381 U.S. at 484 (explaining that the Bill of Rights has "penumbras," which create "zones of privacy" through the First, Third, Fourth, Fifth, and Ninth Amendments). See generally Gormley, supra note 37, at 1357-91 (tracking the history and development of privacy rights under the Fourth and First Amendments).

A. Constitutional Privacy Protections

The United States Constitution does not expressly grant citizens a right to privacy; however, the Supreme Court has interpreted several amendments in the Constitution to provide such a right against government intrusion.42 The absence of an explicit right to privacy has led to broad interpretations of individual privacy which, in turn, has resulted in a scattered meaning of the protection.43 The Supreme Court has held that the Constitution protects a privacy right for individuals in making certain personal decisions.44 The Supreme Court nevertheless has yet to hold that protection exists for an individual’s right to privacy of personal information; despite this fact, personal privacy has played a key role in the development of the Fourth Amendment protection against government searches.45


42. See FRED H. CATE, PRIVACY IN THE INFORMATION AGE 52 (1997) [hereinafter CATE, PRIVACY] (explaining that although the Constitution lacks an explicit guarantee of a right to privacy, the Supreme Court has interpreted the First, Third, Fourth, Fifth, Ninth, Tenth and Fourteenth Amendments to provide an individual with some privacy protection from government activities); Gindin, supra note 12, at 1185 (noting that although a right to privacy is not specifically guaranteed by the Constitution, the Supreme Court has interpreted the Constitution to protect a right of privacy from governmental interference); cases cited supra notes 39-40.

43. See Cate, supra note 38, at 18 (arguing that the Supreme Court’s interpretation of individual privacy protection is confused and limited when compared to explicit constitutional rights).

44. See supra note 39 and accompanying text (describing Supreme Court decisions that found a right to privacy in making certain intimate personal decisions). It should be noted, however, that the relevant constitutional amendments apply to government intrusion and not to the collection and use of information by private individuals or entities. See CATE, PRIVACY, supra note 42, at 50 (noting that constitutional rights only are protected against government actions and not against private parties). The Thirteenth Amendment prohibition of slavery is the only amendment that applies directly to private parties. See id.

45. See Gindin, supra note 12, at 1185 (recognizing that although there is no constitutional right to privacy of personal information, the Fourth Amendment has been interpreted to provide some information privacy protection); see also JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 18 (1997) (stating that the Supreme Court has explicitly relied on privacy in limiting government searches under the Fourth Amendment).
1. Fourth Amendment Protections

The Fourth Amendment provides an implicit right to privacy by prohibiting unreasonable searches and seizures by the government. The first indications that a right to privacy was imbedded in the Fourth Amendment arose in the late 1800s, when the Supreme Court held that the seizure of thirty-five cases of plate glass constituted a Fourth Amendment violation.

The evolution of an implicit privacy right in the Fourth Amendment continued in the late 1920s, when the Court decided its first electronic surveillance case. In Olmstead v. United States, the Court held that the tapping of a telephone wire by federal authorities did not require a warrant because the Fourth Amendment protects only against physical invasion of a person's home and the wire tap did not constitute a physical trespass. In his dissent, Justice Brandeis argued that due to new technologies, the Fourth Amendment protection against unreasonable searches and seizures must be extended to the interception of communications, even though wire taps did not constitute literal physical trespass. Justice Brandeis noted that changes in technology would enable the government to infringe on an individual's right to be let alone like never before. The Court overruled Olmstead in Katz v. United States and embraced Justice Brandeis's reasoning that a physical trespass was not necessary to

46. See U.S. CONST. amend IV (stating that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

47. See Boyd v. United States, 116 U.S. 616, 617, 638 (1886). In Boyd, the Court stated that the principles of the Fourth Amendment applied not only to the illegal seizure of plate glass, but to "all invasions on the part of the government and its employés of the sanctity of a man's home and the privacies of life." Id. at 630.


49. 277 U.S. 438 (1928).

50. See id. at 466. The Court reasoned that, when using a telephone, a voice is projected over telephone wires that are situated outside of the home; thus, an interception of the defendant's voice on these wires could not constitute an "actual physical invasion of his house." Id.

51. See id. at 471-74 (Brandeis, J., dissenting). Justice Brandeis explained his notion that the framers of the Constitution conferred the "right to be let alone—the most comprehensive of rights and the right most valued by civilized men." Id. at 478.

52. See id. at 473 (Brandeis, J., dissenting) (stating that the government had "[s]ubtler and more far-reaching means of invading privacy" due to new technologies).

53. 389 U.S. 347, 351-53 (1967) (holding that the interception of a telephone conversation in a public telephone booth violates the Fourth Amendment protection against an unreasonable search and seizure).
constitute a Fourth Amendment search and seizure violation. In doing so, the Court recognized an implicit privacy concept in the Fourth Amendment. Justice Harlan, in his concurring opinion, stated that the question to be determined was whether there is a "reasonable expectation of privacy," thus further distancing the Court from the idea that a physical trespass is necessary to constitute an illegal search and seizure. Although individuals using the Internet may have a "reasonable expectation of privacy" of their personal identifiable information, one must keep in mind that the Fourth Amendment does not apply to the collection and use of such information by private sector entities.

2. Informational Privacy

The Supreme Court has yet to hold that the Constitution protects informational privacy; however, the Court did touch upon the issue in Whalen v. Roe. At issue in Whalen was a New York State statute requiring physicians to submit copies of prescriptions for abused drugs to the state so that they could be included in a centralized computer file. Although the Court ultimately upheld the statute at issue, it recognized the right of an individual to have his personal information kept private. The Court also recognized, in dicta, that there is an implicit threat to pri-

54. See id. at 351 (stating that "the Fourth Amendment protects people, not places").
55. See id. at 351-52. Justice Stewart stated: "[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Id.
56. See id. at 360-61 (Harlan, J., concurring). Justice Harlan's "reasonable expectation of privacy" principle was later adopted by a majority of the Court and is presently the standard followed. See Terry v. Ohio, 392 U.S. 1, 9 (1968).
57. See Maureen S. Dorney, Privacy and the Internet, 19 HASTINGS COMM. & ENT. L.J. 635, 639 (1997) (explaining that because the Constitution primarily regulates government action, it does not prohibit the private sector's collection and use of personal identifiable information).
59. See id. at 591 (asking whether a state may record in a centralized computer database the names and addresses of persons who have obtained a doctor's prescription for various drugs with both lawful and unlawful markets).
60. See id. at 598 (holding that the New York State statute was a reasonable exercise of state police power). The Court reasoned that New York had a "vital interest" in maintaining control over the distribution of dangerous drugs. See id.
61. See id. at 598-600 (recognizing two types of privacy interests: (1) avoiding disclosure of personal information, and (2) independence to make certain types of intimate decisions); Gindin, supra note 12, at 1186 (noting that the Court "re-affirmed the right of an individual to have his personal information kept private"). The recognition of a privacy interest in avoiding disclosure of "personal matters" seems to be a first for the Supreme Court. See CATE, PRIVACY, supra note 42, at 63. Though the Court's acknowledgment of this privacy interest in Whalen is a "new creation," this right does not involve a "fundamental" interest. See id.
Privacy when personal information is collected in computer databases. Although the Court recognized a privacy right in the unwarranted disclosure of personal information by the government, it did not extend that right to private activities.

**B. Tort Law Privacy**

Although the Supreme Court has found a right to privacy against government intrusions imbedded in the Constitution, it is the "right to be let alone" described by Warren and Brandeis that serves as the basis of protection from an invasion of privacy by private parties under tort law. Seventy years after the Warren and Brandeis article, William Prosser recognized four distinct torts for the invasion of privacy: 1) intrusion upon one's seclusion, 2) misappropriation of one's name and likeness, 3) publicity that places a person in a false light, and 4) public disclosure of private facts. It is with tort law that privacy of one's personal information is most associated. In reality, however, tort law provides little protection for online users' interest in keeping private their personal identifiable information from being collected over the Internet.

---

62. See Whalen, 429 U.S. at 605. The Court stated that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." Id. It further stated that a right to collect such information is usually accompanied by a "duty to avoid unwarranted disclosures." Id.

63. See CATE, PRIVACY, supra note 42, at 66 (stating that the informational privacy right, as with almost all other constitutional rights, "applies only to government activities").

64. See Warren & Brandeis, supra note 37, at 219 (stating that an invasion of the right to privacy should lead to an "action of tort for damages in all cases").

65. See William L. Prosser, Privacy, 48 CAL. L. REV. 383, 389 (1960). Prosser's categorization of torts for an invasion of privacy was adopted by the Restatement (Second) of Torts:

1. One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
2. The right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another, as stated in § 625B; or (b) appropriation of the other's name or likeness, as stated in § 652C; or (c) unreasonable publicity given to the other's private life, as stated in § 652D; or (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.


66. See DECEW, supra note 45, at 14 (noting that the majority of literature on privacy has focused on informational privacy and its relation to tort law); see also Gormley, supra note 37, at 1357 (stating that tort law privacy can be defined as the "right to be let alone, with respect to the acquisition and dissemination of information concerning the person, particularly through unauthorized publication, photography or media").

67. See CATE, PRIVACY, supra note 42, at 89 (stating that the tort of unreasonable intrusion does not provide much support for information privacy). Section 652B of the
C. Statutory Privacy Protections

The United States currently does not have a single, comprehensive privacy law that governs the collection and use of personal identifiable information, either online or offline, by the public or private sector. In Instead, there are a variety of laws that govern the collection and use of personal identifiable information, each addressing a specific industrial or economic sector, or applying only to the government.

1. Legislation Governing the Public Sector

Despite the fact that the Federal Government is arguably the largest collector and user of personal identifiable information in the world, con-

Restatement (Second) of Torts requires that the invasion be "upon the solitude or seclusion of another or his private affairs or concerns" and "highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (1977).

The tort of misappropriation applies only to information privacy in limited instances because it is restricted to the unauthorized commercial use of a "name or likeness of another." See id. § 652C. Although one's name may be the epitome of personal privacy, this tort primarily protects individuals against the use of one's name or likeness in an advertisement or some form of public commercial use without that person's consent. See Dorney, supra note 57, at 642 (explaining that claims under the tort of misappropriation often involve celebrities fighting the unauthorized use of their name or photograph). This tort would have limited application to the collection of personal identifiable information over the Internet; it probably would apply only to cases in which unauthorized use of an individual's name or likeness was used in an Internet advertisement. See id. (stating that "[t]his form of privacy would be implicated if an individual's name or likeness was published on the Internet for commercial purposes without his or her consent"); see also Cate, supra note 38, at 29-30 (noting that the tort of appropriation is of limited value to information privacy).

The other two identified privacy torts also have little to do with the collection and use of private information in the online environment because, like the tort of misappropriation, they concern the public disclosure of individual information. See CATE, PRIVACY, supra note 42, at 90 (arguing that the tort of public disclosure of facts regarding someone's private life "applies only when there is a disclosure to a large audience of private information," and the false light tort requires a publication of knowingly false and offensive private information). It is the private use of personal identifiable information that is at the heart of the online privacy debate, not whether such information is distributed to the general public; therefore, these torts provide "little protection for information privacy." Id.; see also supra notes 9-14 and accompanying text (discussing collection practices and uses of personal identifiable information by the business community).

68. See Dorney, supra note 57, at 642 (noting that the there is no omnibus privacy law in the United States regarding personal information).

69. See infra Parts I.C.1-2 and accompanying notes (discussing United States laws governing the collection, use, and disclosure of personal identifiable information and the industry to which they apply); see also CATE, PRIVACY, supra note 42, at 99 (stating that United States informational privacy laws apply only to specific categories of information users); Gindin, supra note 12, at 1196 (explaining that Congress' approach to protection of personal identifiable information has resulted in "piecemeal" legislation that addresses only specific privacy needs).
trols on its collection and dissemination practices are limited. The major statutes that focus on government conduct pertaining to the collection, use, and disclosure of personal identifiable information are the Privacy Act of 1974 and the Freedom of Information Act (FOIA). These statutes, to the extent that they deal with citizen information, are not limited in scope to preclude information collected over the Internet.

The Privacy Act of 1974 requires that federal agencies collecting personal information for government records must (1) collect only personal information that is relevant and necessary to accomplish a mandated agency purpose; (2) maintain the accuracy of the information; and (3) establish procedures to protect the security of the information. The Privacy Act also prohibits federal agencies from disclosing federal agency records containing personal information without written consent, unless they are used for law enforcement purposes or to protect the health or safety of the individual to whom the records pertain.

The FOIA, which allows individuals to obtain access to Federal agency records, protects informational privacy by exempting certain records.

70. See CATE, PRIVACY, supra note 42, at 76-79 (noting that although the government gathers the largest amount of information in the world, "[p]rivacy-based controls on the government's collection and use of data, outside of the criminal investigation and prosecution context, are very limited").
73. See PERRITT, JR., supra note 3, § 3.16, at 120 (arguing that the scope of the Privacy Act depends on its definition of a "record," not how the record is obtained).
74. The Privacy Act defines a record as any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
76. See id. § 552a(b)(7).
77. See id. § 552a(b)(8).
78. See 5 U.S.C. § 552(b)(1)-(9) (1994) (describing the nine exemptions that prevent
The FOIA applies to all records held by administrative agencies, including any records obtained by an agency through the Internet. To protect the right of privacy, the FOIA specifically exempts the public from obtaining an individual's personnel and medical files, and law enforcement records. The primary application of the FOIA with reference to the Internet is that, like the Privacy Act, it includes government records obtained electronically.

Although the government, as a single entity, may rank first in the collection and use of personal identifiable information, the combined collection activities of the private sector far outweigh the collection practices of the government.

2. Legislation Protecting Informational Privacy in the Private Sector

Congress has addressed the private sector's collection, use, and disclosure of personal identifiable information through the passage of legislation that targets specific industries. For instance, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to protect some forms of electronic privacy and the Fair Credit Reporting Act (FCRA) to govern the collection and disclosure of personal information in the credit reporting industry. Congress has gone as far as regulating the personal information practices of the video rental industry and cable...
television industry; however, the application of these statutes to information collected over the Internet is unclear.

For example, Congress enacted the ECPA to protect private electronic communications from unauthorized access, interception, or disclosure by the government, individuals, or third parties. The ECPA requires that the government obtain a court order before searching an electronic communication. The ECPA provides exceptions, however, allowing for the interception and disclosure of electronic communications in certain circumstances. The most glaring exception, which has a direct effect on personal identifiable informational collection and disclosure, is that only one party to the communication needs to consent to disclosure.

In 1970, Congress passed the FCRA to provide guidelines to credit reporting agencies regarding the dissemination of personal information where consent of the individual has not been obtained. A credit agency may distribute a credit report containing personal identifiable information in order to determine the individual's eligibility for credit, insurance, employment, or for other legitimate business needs. The FCRA requires credit agencies to use reasonable measures to assure the accuracy of such information. 

89. The vast majority of these federal statutes do not solve the privacy problems presented by the Internet because they only govern the disclosure of personal identifiable information, and not the collection or use of such information. See CATE, PRIVACY, supra note 42, at 99 (observing that "[p]rivacy laws in the United States most often prohibit certain disclosures, rather than collection, use, or storage, of personal information"). This lack of regulation of the collection practices of personal identifiable information poses a significant danger to the protection of online privacy when one considers the relative ease of collecting such information over the Internet. See FTC STAFF REPORT, supra note 8, at 1 (noting that because the Internet “mak[es] it even easier and less expensive to gather, store, analyze, transmit, and reuse personal information,” personal privacy may be jeopardized).
91. See 18 U.S.C. §§ 2516, 2518, 2703(b)(1)(B)(ii). Title I of the EPCA restricts the interception of electronic communications while in transit, see id. §§ 2510-2522, while Title II governs the unlawful access and disclosure of stored information. See id. §§ 2701-2709.
92. See 18 U.S.C. §§ 2511(2)(a)-(h), 2701(c), 2702(b).
93. See id. § 2511(2)(c).
95. See id.
of the information. Credit reporting activities that take place over the Internet are fully protected by the FCRA.

In addition, Congress has acted to protect consumers' informational privacy in the videotape rental industry by enacting the Video Privacy Protection Act of 1988 (VPPA) to regulate disclosure of videotape rental information. The VPPA requires informed written consent of the customer in order to disclose information related to that customer's video rentals.

In 1984, Congress enacted the Cable Communications Policy Act (CCPA), requiring cable companies to provide their customers with annual notice as to how their personal identifiable information is used. The CCPA also mandates that the companies provide customers with the general purpose for which any personal identifiable information is collected. Finally, the CCPA requires that customers have the opportunity to remove their name from any mailing list before any such list is sold or otherwise distributed to a third party.

The CCPA may play a role in Internet privacy as more and more online customers gain access to the Internet through cable modems, as

96. See id. § 1681e(b). The FCRA also requires credit reporting agencies to establish a dispute settlement procedure to investigate consumer disputes concerning the accuracy of personal identifiable information in a credit report. See id. § 1681i.


98. See 18 U.S.C. §§ 2710-2711 (1994). It is rumored that outrage over a Washington D.C. newspaper's reporting of the videotape rental preferences of Judge Robert Bork during his failed Supreme Court Justice confirmation Hearing led to the passage of the VPPA. See Cate, supra note 38, at 26 (stating that the VPPA resulted from the disclosure of a list of Judge Bork's video rentals); Dorney, supra note 57, at 646-47.

99. See 18 U.S.C. § 2710(b)(2)(B). The VPPA also requires that personal identifiable information be destroyed within one year of its collection if the original purpose for collecting the information has been satisfied. See id. § 2710(e). There is an exemption in the VPPA that permits the disclosure of viewer habits for marketing and demographic information. See id. § 2710(b)(2)(D)(ii). Under this exception, the customer whose information will be disclosed must be given an opportunity to bar such disclosure. See id. § 2710(b)(2)(D)(i).

100. 47 U.S.C. §§ 521-554 (1994) (regulating the collection, use, and disclosure of personal identifiable information by cable television service providers).

101. See id. § 551(a)(1).

102. See id. § 551(a)(1)(A). Along with a stated purpose, cable service providers must inform customers of the duration of any storage of information, how the customer can obtain access to the information, and the terms of the statute. See id. § 551(a)(1)(C)-(E).

103. See id. § 551(c)(2)(C)(i).

104. A modem is a component of a computer that “convert[s] digital representations of information to analog representations and vice versa.” PERRITT, JR., supra note 3,
opposed to a telephone line, because the Federal Communications Commission (FCC) is attempting to define Internet-based services that are provided by traditional cable operators.\textsuperscript{105} If the FCC decides to define Internet access over cable wires as a "cable service," then consumers who access the Internet through cable wires will receive the privacy protections established in the CCPA.\textsuperscript{106} It should be noted, however, that under the CCPA, such a definition would pertain to the information practices of Internet service providers and not to those of commercial Web sites.\textsuperscript{107}

II. PRIVACY IN THE ONLINE ENVIRONMENT

The United States approach to protecting privacy in the information age, as demonstrated above, is sectoral.\textsuperscript{108} This approach stems from the idea that "[i]nformation privacy is not an unlimited or absolute right."\textsuperscript{109} Rather, the belief is that a balance must be struck between an individual's desire to maintain his privacy and society's enjoyment of the bene-

\textsuperscript{105} See generally Esbin, supra note 104, at i, 83-110 (discussing whether access to the Internet over cable should be described as a "cable service" or "information service").

\textsuperscript{106} See id. at 107-08 (concluding that if Internet service carried over cable is deemed a "cable service," then "customer information and privacy interests" would be governed by the CCPA); Carl S. Kaplan, Cable TV Privacy Law May Protect Web Surfers, CYBER L.J., ¶ 6 (Sept. 11, 1998) <http://www.nytimes.com/library/tech/98/09/cyber/cyberlaw/11law.html> (stating that a consequence of the FCC defining Internet over cable as a "cable service" would be the application of the strict privacy provisions of the CCPA); see also supra notes 100-03 and accompanying text (discussing the consumer privacy protections of the CCPA).

\textsuperscript{107} See Kaplan, supra note 106, at ¶¶ 9-18 (acknowledging that, although Internet service providers using cable lines to provide Internet access would be bound by the cable privacy laws, whether those Internet service providers would be obligated to prevent Web sites from tracking consumer activities remains unclear).

\textsuperscript{108} See discussion supra Part I.C (noting that the legislation to protect privacy in the United States applies only to certain sectors of the government and industry and does not govern information over the Internet as a whole).

\textsuperscript{109} Options Paper, supra note 19, at 6-7 (stating that individuals cannot control personal information that is used for permissible, lawful purposes).
fits associated with the use of his personal information. The Clinton administration contends that industry self-regulation is the best means of protecting the personal privacy of online users without burdening industry with government interference. The idea behind this approach is that the private sector has played a vital role in the growth of the Internet and therefore should continue to lead through "self-regulation wherever appropriate." President Clinton articulated this laissez-faire approach when describing the role of government in the development of "new protections" to protect individual privacy online: "We [the administration] believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation." To assist the private sector to develop effective self-regulatory regimes, the President directed the Secretary of Commerce and the Director of the Office of Management and Budget to work with industries to develop mechanisms to protect privacy using traditional fair information privacy practices.

While the United States is relying on the industry to protect online privacy, both the EU and Canada have taken more structured steps to ensure the protection of their citizens' right to privacy in the online environment. The EU's Data Privacy Directive went into force in October 1995.

110. See FRAMEWORK, supra note 4, at 16 (concluding that only by balancing individual privacy rights and the benefits gained from a free flow of information, will electronic commerce over the Internet succeed); OPTIONS PAPER, supra note 19, at ii (arguing that the question of how to balance privacy with the free flow of information is a critical inquiry in solving the Internet privacy debate).

111. See FRAMEWORK, supra note 4, at 18 (explaining that the private sector should take the lead to protect privacy over the Internet through self-regulatory regimes); Andrews, supra note 23, at A1 (stating that the Clinton administration policy to protect privacy online calls for industries to self-regulate).

112. FRAMEWORK, supra note 4, at 4 (acknowledging that the private sector has been responsible for the Internet's expansion).

113. Id. at 19; cf. Remarks at the Morgan State University Commencement Ceremony in Baltimore, Maryland, 33 WEEKLY COMP. PRES. DOC. 727, 731 (May 18, 1997) (stating that "new protections for privacy in the face of new technological reality[ies]" must be developed).


115. See Bill C-54, supra note 35; EU Data Privacy Directive, supra note 31; CSA
1998, and requires Member States to pass legislation regarding detailed privacy protections in the collection and use of personal identifiable information.\(^{116}\) Additionally, Canada is considering legislation that will codify the Canadian Standards Association's *Model Code for the Protection of Personal Information* to protect the privacy of its citizens online.\(^{117}\)

A. Developing Fair Information Practice Principles in the United States

The mid-1970s saw a growth of automated data processing and record keeping in the United States as the benefits of the computer began to be realized.\(^{118}\) In a response to this growth, the Department of Health, Education, and Welfare’s Advisory Committee on Automated Personal Data Systems developed “fair information practices” governing the collection and use of personal identifiable information.\(^{119}\)

As automated data processing and record keeping practices caught on in other nations, considerations of privacy protections regarding information collection prompted the OECD, in 1980, to recommend its own set of voluntary, international principles governing personal identifiable information.\(^{120}\) The OECD issued *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Privacy Guidelines" or "Guidelines") in an attempt to harmonize different nations' privacy legislation pertaining to the collection and use of personal identifiable information.\(^{121}\) Following the issuance of the *Guidelines*, the personal

---


\(^{117}\) See Bill C-54, supra note 35, at pt. 1, at cls. 5-9 (codifying and defining the obligations of organizations to protect personal information). Bill C-54 states that “every organization shall comply with the obligations set out in Schedule 1.” Id. at cl. 5. As Schedule 1 is a reprint of the principles set forth in the *CSA Model Code*, Bill C-54 codifies the Code’s principles. See id. at pt. 6, sch. 1; see also CSA MODEL CODE, supra note 34 (developing a voluntary standard for the protection of personal information in the global information economy).

\(^{118}\) See *OPTIONS PAPER*, supra note 19, at 1-2 (stating that means of collecting and storing information were increasing in the 1970s).

\(^{119}\) See *HEW REPORT*, supra note 114, at 40-41; *OPTIONS PAPER*, supra note 19, at 1 (observing that the Department of Health, Education, and Welfare established these principles to ensure individuals their right to participate in the collection and use of their personal identifiable information).

\(^{120}\) See generally OECD PRIVACY GUIDELINES, supra note 27 (establishing fair information practice principles in an attempt to both balance individual privacy interests and prevent international interruptions in the free flow of information).

\(^{121}\) See id. at 5 (noting that disparities in national legislation could hamper the free
computer industry boomed, furthering the ability of the public and private sectors to collect and use personal identifiable information. The emergence of the Internet in the 1990s as an easier and more cost efficient means of collecting and using personal identifiable information led to a new round of debate regarding the implementation of fair information practice principles. In the United States, the Information Infrastructure Task Force’s (IITF) Privacy Working Group issued a set of privacy principles similar to those articulated by the OECD, in order to establish fair information practices in the online environment. The Federal Trade Commission (FTC) also articulated fair information practice principles to govern the collection and use of personal identifiable information over the Internet. Finally, the National Telecommunications and Information Administration (NTIA) of the Department of Commerce listed a set of principles of fair information practices in describing the elements of an effective self-regulatory regime to protect online privacy.

flow of information). The OECD Privacy Guidelines established principles that could either be built into existing legislation, or serve as the basis for new legislation governing privacy of personal identifiable information. See id.

122. See FTC Staff Report, supra note 8, at 1 (explaining that the government, industry, and consumers obtained the ability to access a tremendous amount of information with the “personal computer revolution” of the 1980s); Options Paper, supra note 19, at 2 (citing rapid advancement in computer technology and the integration of the telecommunications and data processing industries in the years following the OECD Privacy Guidelines as the cause for an increase in the way in which personal identifiable information was compiled by the government and private industry).

123. See FTC Staff Report, supra note 8, at 1 (noting that the emergence of the Internet in the 1990s and its continued growth may jeopardize individual privacy); Options Paper, supra note 19, at 2 (citing advances in the information technology industry as a primary reason for the emergence of concerns regarding information privacy). See generally U.S. Dep’t of Commerce, Privacy and Self-Regulation in the Information Age (1997) (compiling papers from industry, public interest groups, and academia that explore the issue of privacy over the Internet).

124. See supra note 24 (discussing the role of the IITF). The Privacy Working Group is an advisory group that was created by the IITF to “develop[] proposals to protect individual privacy despite the rapid increase in the collection, storage, and dissemination of personal data in electronic form.” IITF Information Policy Committee (last modified July 11, 1996) <http://www.iitf.nist.gov/ipc/ipc.html>.

125. See Privacy Working Group, Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information 2-3 (1995) [hereinafter IITF Principles] (stating that the IITF principles are intended to be consistent with previously stated guidelines such as those articulated by the OECD), available at <http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivprin_final.html>.

126. See FTC Privacy Report, supra note 9, at 7-11 (outlining fair information practice principles for the collection and use of personal identifiable information).

127. See Elements of Effective Self Regulation for the Protection of Privacy, 63 Fed.
1. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Although the Department of Health, Education, and Welfare already had promulgated informational privacy principles in 1973, the United States participated in negotiations and endorsed the OECD Privacy Guidelines. Citing new computer and communications technologies as the reason for the increased collection and flow of information between countries, the OECD created the Guidelines to balance individual privacy with the free flow of information across borders. The Guidelines were developed to "represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."

There are eight basic principles of the OECD Privacy Guidelines: (1) collection limitation, (2) data quality, (3) purpose specification, (4) use limitation, (5) security safeguards, (6) openness, (7) individual participation, and (8) accountability.

---

128. See HEC REPORT, supra note 114, at 40-42 (explaining a set of fair information principles to protect privacy interests in light of the increased use of record-keeping).

129. See OPTIONS PAPER, supra note 19, at 1 (stating that both the United States Government and several businesses endorsed the OECD Privacy Guidelines).

130. See OECD PRIVACY GUIDELINES, supra note 27, at 5 (stating that there is a need to prevent violations of fundamental human privacy rights and undue restrictions on the free flow of data that is vital to certain sectors of the economy).

131. Id.

132. See id. at 10 (explaining that there should be limits on the collection of information, that the information should be collected lawfully and fairly, and that personal information should be collected with the knowledge or consent of the individual who is the subject of the collection).

133. See id. (recommending that personal information be relevant to the purpose of its use, and that the information should be correct, complete, and current).

134. See id. (calling for the collector of the information to disclose the purpose for which the information is gathered no later than at the time of collection, and requiring the collector to limit any subsequent use to the stated purpose or, if it is used for a different purpose, to state that new purpose).

135. See id. (stating that information should not be disclosed for purposes other than the specified purpose, unless consent of the individual is obtained or the collector is authorized by law to do so).

136. See id. (recommending that security safeguards be established to prevent the loss of, unauthorized access to, tampering with, or disclosure of the information).

137. See id. at 11 (asking members to establish an openness policy so individuals may track developments, practices, and policies of information collection and use).

138. See id. This principle entitles individuals to obtain from an information collector
In 1998, the OECD revisited the OECD Privacy Guidelines to determine whether they are applicable to the electronic environment, focusing specifically on protecting privacy over the Internet. Noting that the Internet is intensifying individual privacy concerns about the collection of personal identifiable information, the OECD recommended that countries reaffirm and apply the Guidelines to the Internet and any other future global computerized networks. OECD Member States also adopted a Declaration on the Protection of Privacy on Global Networks to reaffirm their commitment to the protection of privacy over the Internet.

2. The IITF, the FTC, and the NTIA

In 1995, the IITF's Privacy Working Group issued a report recom
mending a set of principles to build on the *OECD Privacy Guidelines* and to govern the collection and use of personal identifiable information over the Internet.\(^\text{143}\) "[T]he Principles are intended to be consistent with the spirit of current international guidelines, such as the OECD Guidelines regarding the use of the personal information."\(^\text{144}\) In articulating its principles, the IITF believed that it was the responsibility of the government, industry, and individuals to protect the privacy of personal identifiable information.\(^\text{145}\)

The IITF’s report discusses three general principles that apply to all Internet participants: (1) information privacy, (2) information integrity, and (3) information quality.\(^\text{146}\) The IITF also established principles specifically for collectors and users of personal information: (1) acquisition,\(^\text{147}\) (2) notice,\(^\text{148}\) (3) protection,\(^\text{149}\) (4) fairness,\(^\text{150}\) and (5) education.\(^\text{151}\) Finally, the IITF describes awareness, redress, and empowerment as principles that should be afforded to individuals who provide personal

---

143. See IITF PRINCIPLES, supra note 125, at 5 (articulating the fair information practice principles that need to be followed in order to ensure continued development of the Internet). The IITF decided that traditional fair information practices, developed in the age of paper records, “must be adapted to a new environment in which information and communications are sent and received over networks by users who have very different capabilities, objectives, and perspectives.” Id. at 4.

144. Id. at 3 (footnote omitted).

145. See id. at 4 (stating that the new principles must acknowledge that all members of society share in the duty to ensure that individuals are treated fairly in the use of their personal identifiable information, regardless of whether that information is in electronic or paper form).

146. See id. at 5. The “Information Privacy Principle” recognizes that an “individual’s reasonable expectation” of privacy should be respected in regard to the collection, disclosure, and use of that individual’s personal information. See id. This “reasonable expectation” may be higher than the level required under Fourth Amendment search and seizure jurisprudence. See id. The information integrity principle states that personal information should be protected from tampering or unauthorized use. See id. The “Information Quality Principle” calls for the collected information to be “accurate, timely, complete, and relevant” to a collector’s stated purpose. See id.

147. See id. at 6 (stating that information users should determine the impact of collection and use of personal information on privacy, and should collect and keep only necessary information).

148. See id. at 6-8 (directing those who collect information to inform individuals of the reasons for the collection, the steps they will take to protect the individual’s interest, the consequences of providing or withholding information, and any possible rights of redress for the misuse of information).

149. See id. at 8 (encouraging information collectors to take steps to protect the individual’s information from subsequent improper disclosure or alterations).

150. See id. at 8-9 (recommending that information collectors either limit the use of the personal information or obtain the individual’s consent).

151. See id. at 9 (stating that information collectors should educate all parties involved about their collection practices).
information.\footnote{See id. at 10-11. In articulating the “Awareness Principle,” the IITF states that individuals have a responsibility to understand any consequences resulting from providing personal identifiable information to others. See id. at 10. As for the “Redress Principle,” the IITF believes that individuals have the right to be protected from any harm caused by improper disclosure or use of personal identifiable information. See id. at 11. The “Empowerment Principle” calls for individuals to be afforded an opportunity to “safeguard their own privacy” by requiring the collector of personal information to provide individuals with a means to access and correct their personal identifiable information. See id. at 10.}

The IITF Principles are actually a step back from the OECD Privacy Guidelines, for they shift some of the responsibility for the protection of privacy over the Internet from the data collectors to the data subjects.\footnote{Compare id. at 10 (describing the “Awareness Principle”), with supra note 138 (discussing the OECD’s “Individual Participation Principle”). The OECD “Individual Participation Principle” states that “[a]n 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,” and, among other things, to have access to any such information. OECD PRIVACY GUIDELINES, supra note 27, at 11. The IITF “Awareness Principle” explains that “individuals should obtain adequate, relevant information” about why and how their personal identifiable information is being used. See IITF PRINCIPLES, supra note 125, at 10. The commentary to this principle states that “[t]he Awareness Principle recognizes that although information collectors have a responsibility to inform individuals why they want personal information, individuals also have a responsibility to understand the consequences of providing personal information to others.” Id.}

This shift is particularly disheartening, not to mention unrealistic, in light of the fact that the Internet permits the gathering of data about an individual with or without the individual’s knowledge.\footnote{See supra notes 9-13 and accompanying text (discussing the means employed by Web sites to track an individual’s personal identifiable information). The IITF position may place an insurmountable burden on the individual who “surfs” the Internet on a regular basis and visits multiple Web sites and multiple Web pages each time he uses the Internet. But cf. IITF PRIVACY PRINCIPLES, supra note 125, at 10 (stating in the Comment section of the “Awareness Principle” that individuals shall not be held responsible for supplying information if they are not given enough information to make an intelligent choice). This problem is especially alarming as a vast majority of Web sites compile personal identifiable information without posting notification on their Web sites to inform the visitor of their information collection practices. See FTC PRIVACY REPORT, supra note 9, at 23, 27 (finding, in a March 1998 survey, that 92% of a sample of 674 Web sites collected personal information, of which only 14% disclosed their information practices).}

The FTC also has been actively involved in addressing the issue of online privacy over the past several years.\footnote{See FTC PRIVACY REPORT, supra note 9, at i-i (reporting on the effectiveness of self-regulation as a means of protecting online privacy through a comprehensive study of the information practices of commercial Web sites); FTC IRS REPORT, supra note 8, at i (studying the information practices of the individual reference service industry); FTC STAFF REPORT, supra note 8, at 1-2 (exploring privacy issues arising out of the emerging online marketplace as well as online consumer privacy protections). See generally Roscoe B. Starek, III & Lynda M. Rozell, The Federal Trade Commission’s Commitment to On-
privacy, the FTC has recognized that governments in the United States and abroad have established "certain core principles of fair information practice."

The FTC concluded that all previous statements of fair information practice principles have in common five core principles: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress. The FTC fair information principles reiterate the core principles of privacy protection in the collection, use, and disclosure of personal information, and build on those articulated in the past by including an enforcement principle in conjunction with a redress principle. Specifically, the FTC recognizes "that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them."

In addition to the IITF and the FTC, the NTIA has responded to the
Presidential Directive to ensure privacy is protected on the Internet by issuing fair information practice principles. The NTIA agreed with the FTC that in order to have effective self-regulatory regimes for the collection and use of personal information online, fair information practices coupled with enforcement mechanisms are needed.

The NTIA considers fair information practices to include (1) awareness, (2) choice, (3) data security, (4) data integrity, (5) consumer access, and (6) accountability. The NTIA considers proper enforcement mechanisms to include (1) consumer recourse, (2) verification, and (3) consequences. The NTIA Principles, like those articulated by the FTC, properly address enforcement concerns, but unlike the FTC do so only in the self-regulatory context, thereby leaving harmed individuals without a private right of action. This requires one to ask whether the private sector truly would provide for an enforcement mechanism within the framework of self-regulation. The United States, led by the

164. See Elements of Effective Self Regulation for the Protection of Privacy, 63 Fed. Reg. 30,729, 30,729-30 (1998) (noting that President Clinton “directed the Department of Commerce and the Office of Management and Budget to work with the private sector to develop and implement effective, consumer-friendly, self-regulatory privacy regimes”); see also supra text accompanying note 24 (quoting the President’s Directive on Electronic Commerce).

165. See Elements of Effective Self Regulation for the Protection of Privacy, 63 Fed. Reg. at 30,731. The NTIA explained that “a self-regulatory privacy regime should include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights...” Id.

166. See id. (stating that privacy policies, notification, and consumer education should be addressed).

167. See id. (stating that consumers should be able to exercise choice as “to whether and how their personal [identifiable] information is used”).

168. See id. (providing that a mechanism should be instituted to ensure security).

169. See id. (stating that companies should keep only information that is relevant for the purpose of collection, and that the information should be “accurate, complete, and current”).

170. See id. (explaining that consumers should have a means to access and correct any false information).

171. See id. (stating that a company should be held accountable for failure to comply with its privacy policy).

172. See id. at 30,731-32 (stating that an enforcement mechanism must be put into place in order to assure compliance with self-regulation).

173. Compare id. (leaving the selection and implementation of an enforcement mechanism to the private sector), with FTC PRIVACY REPORT, supra note 9, at 10-11 (studying enforcement mechanisms and redress possibilities both in self-regulatory regimes and in legislation, which provides for either private rights of action or criminal penalties).

174. See ACLU, LETTER REGARDING THE PROTECTION OF ONLINE PRIVACY III.2 (July 6, 1998) (arguing that the lack of legislative enforcement mechanisms provide “little incentive in a
Clinton administration, seems to believe, at least for now, the most efficient way to protect privacy of personal identifiable information online is through industry self-regulation, and does not appear poised to endorse or implement any statutory or administrative enforcement mechanisms. There is a consensus among international and federal agencies, however, that privacy over the Internet can be protected only by the use of fair information principles.

**B. The EU Data Privacy Directive**

While the United States has continued to rely on self-regulation, the EU approached online privacy by adopting Directive 95/46/EC, more commonly known as the Data Privacy Directive, which sets forth principles for the collection and use of personal identifiable information. The Directive's objective is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

The Directive requires that a gatherer of personal information collect such information for "specified, explicit and legitimate purposes." Ar-
ticle Six of the Directive also requires the information to be adequate and relevant for the stated purpose, accurate and current, and maintained in personal identifiable form for only the amount of time needed to accomplish the stated purpose for collection. The Directive further provides that personal identifiable information can be processed only if the subject of the information gives unambiguous consent.

The Directive also requires collectors of personal information to provide the data subject with notice of their collection practices. Collectors of personal identifiable information must provide the subject of the information with, among other things, the identity of the collector, the purpose of collection, any possible recipients of that information, that there is a mechanism in place to access and correct inaccurate information, and a guarantee of fair processing of the information. The Directive further mandates that the data subject be given a right of access and a right to object to the processing of his information, while requir-

180. See id. art. 6(1)(c)-(e), at 40 (establishing information collection and use principles relating to data quality).

181. See id. art. 7(a), at 40. A data collector may process information without unambiguous consent if the processing is necessary (1) to perform a contract and the data subject is a party to that contract; (2) to comply with a legal obligation; (3) to protect the vital interests of the data subject; (4) to perform "a task carried out in the public interest"; and (5) for legitimate interests of the data collector that would override the individual's fundamental rights and freedoms. See id. art. 7(b)-(f), at 40.

182. See id. art. 10, at 41 (governing the notice requirements for a gatherer of information who obtains the data directly from the data subject); id. art. 11, at 41-42 (governing disclosure of information practices by third parties that do not obtain the information directly from the data subject).

183. See id. art. 10, at 41. The Directive requires that collectors of information must provide identical notice about third parties that obtain the information. See id. art. 11, at 41-42. The information mandated in Articles 10 and 11 are almost identical to the FTC's "Notice/Awareness Principle." Compare id. arts. 10-11, at 41-42, with FTC PRIVACY REPORT, supra note 9, at 7-8 (stating that consumers should be given notice of the collector of the data, the use or purpose of the collection, any potential recipients of the information, and steps taken by the collector to protect the quality of the information).

184. See EU Data Privacy Directive, supra note 31, art. 12, at 42 (requiring collectors of personal identifiable information to provide consumers access to their information "without excessive delay or expense"); cf. FTC PRIVACY REPORT, supra note 9, at 9 (articulating the "Access/Participation Principle," which states that individuals should have the ability to access and contest data in a "timely and inexpensive" way).

185. See EU Data Privacy Directive, supra note 31, art. 14, at 42-43 (requiring that a citizen be granted, upon request and free of charge, the option to not have his personal identifiable information processed). The FTC principles are consistent with the EU Data Privacy Directive with regard to consumer choice or consent. Compare FTC PRIVACY REPORT, supra note 9, at 8-9 (describing the "Choice/Consent Principle"), and supra note 159 (same), with EU Data Privacy Directive, supra note 31, arts. 7(a), 14, at 40, 42-43 (requiring mandatory consent to the processing of personal data and giving a consumer the right to object to the processing of his personal data).
ing that the collector provide for confidentiality and security of the information. 186

Member States must provide judicial remedies for any breach of the privacy rights granted by the Directive. 187 In addition, Article Twenty-five requires Member States to ensure that personal identifiable information is transferred outside of the EU only to countries with "adequate" privacy protection. 188 Whether a non-EU country provides adequate protection will be determined on a case-by-case basis. 189

There has been discussion between members of the EU and the United States over whether the self-regulatory model to protect privacy online used by the United States will satisfy this requirement. 190 How-

186. See EU Data Privacy Directive, supra note 31, arts. 16-17, at 43 (governing the unauthorized processing of personal information and the protection of data from accidental loss and destruction and unauthorized disclosure and access); cf. Hearing on Privacy in Cyberspace, supra note 176, at 308 (statement of Hon. Robert Pitofsky, Chairman, Federal Trade Commission) (describing the FTC "security/integrity" practice principle, which states that a Web site should "be required to take reasonable steps to protect the security and integrity of [personal] information").


188. See id. art. 25, at 45-46. Article 25 has been the subject of much discussion during the implementation of the Directive because it could be a major stumbling block to the continued growth of electronic commerce. See Baker et al., supra note 17, at 49, 51 (noting that Article 29 (which should be Article 25) could harm the hopes of direct marketers to perform target advertising over the Internet, which is a key aspect of the growth of electronic commerce); Robert O'Harrow, Jr., Privacy Rules Send U.S. Firms Scrambling, WASH. POST, Oct. 20, 1998, at C1 (noting that the Directive is leading to anxiety on the part of American businesses because the broad scope of the Directive covers online orders for products).

189. See EU Data Privacy Directive, supra note 31, art. 25(2), at 45-46 (mandating that the level of protection afforded by a non-EU country should be assessed by considering all of the circumstances surrounding the particular data transfer); see alsoSpiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 IOWA L. REV. 445, 464 (1995) (stating that transmission of personal data to a non-EU country presupposes that country provides an "adequate" level of privacy protection for the subject of the data).

190. See Baker et al., supra note 17, at 51 (stating that officials for the United States and the EU are negotiating to prevent a shutdown of transborder data flows that may result due to inadequate privacy protections by self-regulators); see also Ambassador David L. Aaron, Safe Harbor Letter From Ambassador Aaron (visited June 14, 1999) <http://www.ita.doc.gov/ecom/aaron419.html> (discussing ongoing negotiations between the Department of Commerce and the European Commission "to develop clear and predictable guidance to U.S. organizations that would enable them to comply with the requirements of the European Union's Directive on Data Protection regarding personal data transfers to third countries"). See generally Data Protection Working Party, Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country? (visited June 15, 1999) <http://www.europa.eu.int/comm/
ever, with only six of the fifteen EU members passing national legislation to meet the requirements of the Data Privacy Directive, an interruption of data flow between the United States and the EU in the immediate future seems remote.\textsuperscript{191}

\textbf{C. The Canadian Approach}

Canada, like the United States, relies on industry self-regulation to govern the collection and use of personal identifiable information by the private sector.\textsuperscript{192} Canada nevertheless decided to establish a national model standard for the protection of personal information,\textsuperscript{193} in part to

\textsuperscript{191} See Andrews, supra note 23, at A1 (noting that although each member must eventually pass national laws to implement the EU Directive, only six of the fifteen had done so as of the date of the article).

\textsuperscript{192} See Bennett, supra note 33, at 157 (describing Canada's approach to protecting privacy in the private sector as similar to the United States' policy of self-regulation and the implementation of "patchwork" legislation). As mentioned above, Canada currently is considering legislation to codify the Canadian Standard Association's \textit{Model Code for the Protection of Personal Information}. See Bill C-54, supra note 35.

\textsuperscript{193} See CSA \textit{MODEL CODE}, supra note 34, at Introduction (explaining that the
comply with the Article Twenty-five adequacy standard of the EU Data Privacy Directive.\textsuperscript{194} The \textit{Canadian Standards Association (CSA) Model Code for the Protection of Personal Information ("CSA Code" or "Code")} establishes ten practice principles that must be adopted as a whole by those who wish to participate:\textsuperscript{195} (1) accountability;\textsuperscript{196} (2) identifying purposes;\textsuperscript{197} (3) consent;\textsuperscript{198} (4) limiting collection;\textsuperscript{199} (5) limiting use, disclosure and retention;\textsuperscript{200} (6) accuracy;\textsuperscript{201} (7) safeguards;\textsuperscript{202} (8) openness;\textsuperscript{203} (9) individual access;\textsuperscript{204} and (10) challenging compliance.\textsuperscript{205} Although the \textit{CSA Code} is essentially a guideline for a self-regulatory regime, it has allowed Canada to establish a national standard for online privacy protection of personal identifiable information.\textsuperscript{206}

\textit{OECD Privacy Guidelines} served as the basis for the \textit{CSA Model Code}.

194. See Bennett, supra note 33, at 157 (citing the EU Data Privacy Directive as one of many international developments that caused Canadian federal policy-makers to rethink their approach to the protection of personal identifiable information).

195. See \textit{id}. at 158 (noting that organizations must adopt the 10 principles as a whole, and thus, they may not "cherry-pick" only those principles they deem worthy).

196. See CSA MODEL CODE, supra note 34, § 4.1 (stating that an organization, such as any business, is responsible for the information under its control and that it should designate one or more individuals to be held accountable for compliance with the principles).

197. See \textit{id}. § 4.2 (calling for organizations to identify the purposes for which personal identifiable information is collected at or before the time of collection).

198. See \textit{id}. § 4.3 (requiring data subject's knowledge and consent before a collector can use or disclose the collected personal identifiable information, unless inappropriate).

199. See \textit{id}. § 4.4 (limiting the collection of personal identifiable information to what is necessary for the identified purpose of collection, and requiring use of lawful collection methods).

200. See \textit{id}. § 4.5 (limiting the use and disclosure of information to the stated purpose of collection, except where the individual consents; requiring the retention of personal information for only as long as is necessary to accomplish the stated purpose of collection).

201. See \textit{id}. § 4.6 (demanding that personal identifiable information be accurate, complete, up-to-date, and necessary for the stated purpose).

202. See \textit{id}. § 4.7 (calling for the organization collecting information to provide security safeguards "appropriate to the sensitivity of the information").

203. See \textit{id}. § 4.8 (explaining that an organization should be able to provide specific information about its collection and maintenance practices and privacy policies to individuals).

204. See \textit{id}. § 4.9 (requiring organizations collecting information to provide to an individual, upon request, access to the "existence, use, and disclosure" of his personal identifiable information). Under the individual access principle, an individual requesting access to his information should have the opportunity to challenge the information's accuracy and have it amended where appropriate. See \textit{id}.

205. See \textit{id}. § 4.10 (stating that an individual should be able to direct a challenge regarding an organization's compliance with the privacy principles to the organization's designated individual(s) who are responsible for compliance).

206. See Bennett, supra note 33, at 158 (explaining that the \textit{CSA Model Code} enabled Canada to harmonize privacy rules across provinces and sectors, while at the same time avoiding regulation through legislation).
D. Self-Regulatory Efforts in the United States

As Europe and Canada move toward legislation, many companies and industry groups in the United States, such as the direct marketing industry, have expressed strong support for self-regulation to govern the protection of privacy of personal identifiable information.\(^{207}\) Indeed, in response to the Clinton administration's call for self-regulation, several private industry groups have issued guidelines for their members to implement privacy protection in their personal information collection practices.\(^{208}\)

For example, in the banking sector, the Bankers Roundtable has established guidelines for members of the banking industry to institute privacy principles.\(^{209}\) The guidelines set forth eight privacy principles: (1) the recognition of a customer's expectation of privacy,\(^{210}\) (2) use, collection, and retention of customer information,\(^{211}\) (3) maintenance of accurate information,\(^{212}\) (4) limiting employee access to information,\(^{213}\) (5)\(^{207}\) See Andrews, \textit{supra} note 23, at A1 (noting that many companies have lobbied against legislation to regulate information collection practices); O'Harrow, Jr., \textit{supra} note 188, at C1 (discussing the industrial sector's desire to avoid legislation regulating data collection). Leading the efforts in support of self-regulation is the direct marketing industry, whose companies make money through the collection and use of information. \textit{See Hearing on Privacy in Cyberspace, supra} note 176, at 335 (statement of Jerry Cerasale, Senior Vice President of Government Affairs for the Direct Marketing Association) (noting that Direct Marketing Association member companies have a tremendous stake in the future of the Internet and electronic commerce and that the group believes that self-regulation is the most effective method to protect online privacy).

\(^{208}\) See \textit{Banking Industry Technology Secretariat, The Bankers Roundtable, Privacy Principles Implementation Plan} [hereinafter \textit{Banking Principles}] (establishing the banking industry's information practice privacy principles regarding personal identifiable information), \textit{reprinted in FTC Privacy Report, supra} note 9, at app. E; \textit{Individual Reference Services Group, Individual Reference Services Industry Principles} (1997) [hereinafter \textit{IRS Principles}] (setting guideline principles for individual reference service industry members), \textit{reprinted in FTC IRS Report, supra} note 8, at app. D; \textit{The Direct Marketing Association, Marketing Online: Privacy Principles and Guidance} [hereinafter DMA Principles] (describing principles for direct marketers to follow when collecting, using, and disclosing personal identifiable information), \textit{reprinted in FTC Privacy Report, supra} note 9, at app. E; \textit{see also} \textit{FTC Privacy Report, supra} note 9, at app. E (containing copies of nine industry-specific guidelines provided to the FTC by the individual industries).

\(^{209}\) See \textit{Banking Principles, supra} note 208.

\(^{210}\) See \textit{id.} at 3 (stating that financial institutions should respect customers' privacy expectations and explain the bank's privacy practices to consumers). The guidelines ask that banks approve a plan implementing the principles, and that they develop a mechanism for communicating their policies to customers. \textit{See id.} at 1.

\(^{211}\) See \textit{id.} at 3 (explaining that financial institutions should collect, retain, and use personal identifiable information only to aid the organization's business and to provide customers with products and services).

\(^{212}\) See \textit{id.} (calling for the establishment of procedures to ensure that the consumer's
protection of information via established security procedures, (6) restrictions on the disclosure of account information, (7) maintaining customer privacy in the bank's business relationships with third parties, and (8) disclosure of privacy principles to customers. The guidelines also require the banks to set up internal mechanisms to assure compliance, address breaches, and maintain accuracy of customer information. Although the Bankers Roundtable guidelines address the five basic fair information practice principles articulated by the FTC, they lack the FTC's commitment to a uniform enforcement procedure; instead, they rely on the internal procedures of each bank to enforce the practices of the bank.

Another industry group to provide its members with online privacy principles and information practice guidance is the Direct Marketing Association (DMA). The DMA guidelines call for marketers operating Web sites to post an easy to find notice to consumers of the marketer's
information collection practices, and to provide consumers with an opportunity to prohibit disclosure of their information. The DMA guidelines, however, do not provide data subjects with other basic protections cited by the FTC, including access to the individual’s information and the assurance that the information is secure and accurate. Additionally, the DMA guidelines fail to provide an enforcement mechanism should a breach of policy arise.

In addition to the Bankers Roundtable and the DMA, the Individual Reference Services Group (IRSG) has articulated a set of industry principles applicable to the collection and use of personal identifiable information. The principles include (1) education, (2) acquisition of information from reputable sources, (3) accuracy, (4) security, (5) openness, (6) choice, and (7) access. Unfortunately, the IRSG guidelines also serve as another example of a self-regulatory regime that is lacking any, yet alone effective, enforcement mechanisms.

222. See id. at 3 (stating that all marketers with an online Web site should disclose information collection and use practices to consumers on the Web site and should provide consumers with the opportunity to prohibit the disclosure of such information).

223. Compare DMA PRINCIPLES, supra note 208, with FTC PRIVACY REPORT, supra note 9, at 9-10 (discussing the “Access/Participation Principle” and the “Integrity/Security Principle”).

224. See DMA PRINCIPLES, supra note 208 (guiding DMA members to provide online customers with the notice of their collection practices as well as an opportunity to opt out of any disclosure of individual information but failing to mention any need for enforcement mechanisms). This is disturbing because, as mentioned above, the FTC has stressed that “core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.” FTC PRIVACY REPORT, supra note 9, at 10; see also supra note 176, at 346 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology (arguing that “[w]ithout a strong commitment to ensuring adherence to policies, self-regulation is doomed to be inadequate’’)).

225. See IRS PRINCIPLES, supra note 208.

226. See id. at 2. The IRSG avows that its members should make efforts to educate the public about their privacy policies and the benefits of the free flow of information. See id.

227. See id. (recommending that members acquire personal identifiable information only through reputable sources in the government and private sectors).

228. See id. (explaining that members should take all reasonable steps to assure the accuracy of the personal identifiable information).

229. See id. at 5 (requiring members to maintain systems to prevent unauthorized access to stored information).

230. See id. (stating that members shall provide notice of their information collection practice to consumers through Web sites, advertisements, or educational efforts).

231. See id. (requiring member companies, upon request, to provide consumers with available options to limit use or disclosure of their personal identifiable information).

232. See id. at 6 (providing individuals, upon their request, with their personal identifiable information that is held by the member company).

233. See id. at 2-6 (showing the absence of enforcement mechanisms in the discussion of information practice policies protecting privacy in the IRSG industry); cf. Hearing on
Finally, the Interactive Services Association (ISA) provides principles for online information collection by online operators and by Internet and online service providers.\(^{234}\) The ISA principles require that notice of a privacy policy be posted on Web sites, and that it be easy to find, readable, and understandable.\(^{235}\) Furthermore, if an Internet or online service provider intends to disclose information to third parties for commercial purposes, the customer should be given the means to exercise a choice as to whether he wants that information disclosed.\(^{236}\) Like the DMA principles, the ISA principles fail to provide online users with access to their information, any security assurances, or an enforcement mechanism.\(^{237}\)

**E. Other Industry Led Efforts to Protect Privacy**

In addition to efforts by individual industry trade groups to establish fair information practice principles, there have been several other industry initiatives to establish and enforce fair information practice principles over the Internet.\(^{238}\)

One such program, TRUSTe, is a nonprofit initiative sponsored by companies such as Microsoft, IBM, AT&T, Excite and Compaq, that provides oversight functions to ensure that its members are following

---

\(^{233}\) See Interactive Serv. Ass'n, Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators (1997), reprinted in FTC Privacy Report, supra note 9, at app. E.

\(^{234}\) See id. The notice should state what information is being collected, how it is collected, the purpose for the collection, and how a customer may limit the disclosure of his or her personal identifiable information. See id.

\(^{235}\) See id. (requiring industry members to provide consumers with notice of their collection practices and a choice to online users to prevent disclosure of their information to third parties but not suggesting any enforcement regime); see also supra notes 223-24 and accompanying text (discussing the failure of the DMA to include in its basic fair information practice principles any reference to user access to their information, security assurances, or an enforcement mechanism).

\(^{236}\) See Better Business Bureau, BBBOnline® FAQs (visited Mar. 30, 1999) <http://www.bbbonline.com/about/FAQs.html> (discussing the BBBOnline Privacy program, which “awards seals to online businesses that have been verified to be following good information practices”); TRUSTe, How the TRUSTe Program Works (visited Mar. 30, 1999) <http://www.etrust.org/webpublishers/pub_how.html> (establishing an online seal program with a goal to provide Internet users “with control over their personal information”); see also Will Rodger, Pretty Lame Privacy, Bus. 2.0, Sept. 1998, at 38 (critiquing various industry led initiatives to protect privacy over the Internet).
their posted privacy policies. Companies from any industry wishing to participate in the program work with TRUSTe to form an online privacy policy conforming to certain principles that will be posted on the company Web site. To obtain a “trustmark,” TRUSTe members must post an easy to locate, read, and understand privacy statement, giving visitors to the Web site notice that the company is a licensee of the TRUSTe program. In its privacy statement, a TRUSTe licensee must provide notice of the company’s information collection practices. The TRUSTe program also requires licensees to provide visitors with an opportunity to exercise the choice to prohibit the site from passing their personal identifiable information to a third party.

TRUSTe monitors its members through random Web site checks to ensure that members are adhering to their stated privacy policies. A breach of policy may result in “revocation of the trustmark, termination from the TRUSTe program, breach of contract proceedings, or referral

239. See TRUSTe, We're Building a Web You Can Believe In! (visited Mar. 30, 1999) <http://www.etrust.org/about/> (stating that TRUSTe is a “nonprofit privacy initiative” that provides an oversight program to establish Web site credibility); TRUSTe, TRUSTe Sponsors (visited Mar. 30, 1999) <http://www.etrust.org/about/about_sponsors.html> (listing the sponsors of the TRUSTe program to protect privacy online).

240. See TRUSTe, TRUSTe Program Principles (visited Mar. 30, 1999) <http://www.etrust.org/webpublishers/pub_principles.html> (stating that TRUSTe provides companies with insight to ensure that companies post an effective privacy policy on the company’s Web page that complies with fair information practices). Web sites that meet TRUSTe privacy principles will be given a TRUSTe “trustmark” in exchange for a licensing fee. See id.; TRUSTe, How to Join the TRUSTe Program (visited Mar. 30, 1999) <http://etrust.org/webpublishers/pub_join.html> (listing the annual licensing fees of the TRUSTe program).

241. See TRUSTe, TRUSTe License Agreement Rev 4.3 (last modified Mar. 3, 1999) <http://www.etrust.com/webpublishers/pub_agreement.html> [hereinafter TRUSTe License Agreement] (stating that licensees must maintain and adhere to the privacy statement that is written by the company and approved by TRUSTe).

242. See id. at 1(E). Specifically, TRUSTe requires the company to post: (1) what information is collected; (2) who is collecting the information; (3) how the information is used; (4) with whom the information will be shared; (5) choices available to the visitor of the site regarding collection and use; (6) the types of security procedures in place to protect information; and (7) whether visitors may access and correct their information. See id.

243. See id. at 1(F). This choice is available when “such use or distribution is unrelated to the purpose for which the information was collected.” Id.

244. See TRUSTe, The TRUSTe Program: How it Protects Your Privacy (visited Mar. 30, 1999) <http://www.etrust.org/users/users_how.html> (observing that Web sites that display the “trustmark” must agree to comply with oversight procedures to determine company compliance with the program). TRUSTe also monitors its members by requiring compliance reviews by a CPA firm, and through “[f]eedback and complaints from the online community.” Id.
to the appropriate federal authority,” depending on the severity of the breach. 245

Similar to the TRUSTe program, the Better Business Bureau (BBB) launched the BBBOnline Privacy Program (“BBB Program”) that awards seals to companies that follow specified privacy principles. 246 To qualify for a “BBBOnLine Privacy Seal” a company must adopt and implement a privacy policy to be posted on the company’s Web site, the company must be in good standing with the BBB, and the “website or online service must be intended to be directed at United States residents.” 247

To be eligible for the BBB Program, a company must provide notice to consumers via an easy to read privacy policy that discloses, among other things, the identity of the collector, the type of information collected, and how it will be used. 248 The BBB Program also requires participating Web sites to implement a procedure that allows individuals to prohibit uses of their information that are unrelated to the stated purpose of collection. 249 Finally, the program participants must assure that the information they have collected is accurate, and that individuals have the ability to access their information to correct inaccuracies. 250

The BBBOnLine Privacy program also furnishes a dispute settlement system to consumers who have complaints about a participant’s information practices. 251 Should a company continue to violate its own privacy

245. Id. (describing the consequences of a breach of TRUSTe policy).
246. See supra note 238 (discussing the BBBOnLine Privacy program). The BBBOnLine Privacy program is sponsored by such companies as AT&T, Eastman Kodak, Microsoft, and Sony Electronics. See Better Business Bureau, BBBOnLine® Corporate Sponsors (visited Mar. 30, 1999) <http://www.bbbonline.com/about/corpsponsors.html> (listing those companies that have provided financial support to assist BBBOnLine).
248. See id. (listing the minimum components of the required privacy policy). The site must also disclose any choices that an individual has regarding the collected information, and the procedures the site will take to ensure security, accuracy, and access to the personal information. See id.
249. See id. The company also “must provide individuals with a choice regarding the transfer of information to third parties for marketing purposes.” Id.
250. See id. (stating that the “seal participant must establish effective and easy to use mechanisms to permit individuals access to correct inaccurate factual information”).
251. See Better Business Bureau, BBBOnLine® Online Privacy Self-Regulation Program (visited Mar. 30, 1999) <http://www.bbbonline.com/businesses/privacy/self-regulation.html> (discussing the program’s enforcement mechanisms). Following a consumer complaint and before using the dispute settlement procedure, the BBB will encourage the individual and the company to resolve the complaint on their own. See Better Business Bureau, supra note 238 (responding to a question asking about the procedures to handle a
statement, it will face having its seal revoked, "will be publicly identified," and possibly will be referred to the appropriate Federal agency. The BBB Program promises to "monitor compliance through rigorous requirements for participating companies to undertake, at least annually, an assessment of their procedures and data collection and distribution practices."  

III. PROBLEMS WITH THE UNITED STATES POLICY OF PURE SELF-REGULATION TO PROTECT PRIVACY ONLINE

Despite the considerable efforts of the private sector to implement self-regulatory regimes, a policy of pure self-regulation to govern privacy over the Internet has some fundamental flaws. For instance, the scope of voluntary guidelines usually does not extend past that of a particular industry promulgating such guidelines, leaving most Web sites outside of the coverage of self-regulatory regimes.

Another problem with a policy of self-regulation is the difficulty of monitoring whether companies are adhering to the principles defined

252. See Better Business Bureau, supra note 238.

253. Hearing on Privacy in Cyberspace, supra note 176, at 326 (statement of Steven J. Cole, Senior Vice President and General Counsel, Council of Better Business Bureaus). Although not a seal program like TRUSTe or BBBOnline, the Online Privacy Alliance is a multi-industry coalition consisting of over 80 companies "committed to promoting the privacy of individuals online." Online Privacy Alliance, Frequently Asked Questions (visited Mar. 29, 1999) <http://www.privacyalliance.org/facts>. Members of the Online Privacy Alliance agree to adopt and implement a privacy policy that provides online users with notice of information collection practices, the ability to exercise a choice as to how their information is used, data security, data quality, and access to their personal identifiable information. See Online Privacy Alliance, Guidelines for Online Privacy Policies (visited Mar. 29, 1999) <http://www.privacyalliance.org/resources/ppguidelines.shtml>.


255. See Hearing on Privacy in Cyberspace, supra note 176, at 307 (statement of Hon. Robert Pitofsky, Chairman, Federal Trade Commission) (stating that "it will be difficult for self-regulatory programs to govern all or even most commercial Web sites"); see also id. at 311 (statement of Hon. Mozelle W. Thompson, Commissioner, Federal Trade Commission) (arguing that self-regulatory regimes are finding it difficult to overcome the inability to gain wide-spread coverage of privacy protection online). The FTC notes that "[i]ndustry self-regulation has only been endorsed and adopted by a small percentage of the actual online community." Id. (noting that most self-regulatory initiatives have focused on the most popular Web sites).
The absence of a system to effectively monitor a company enables the company to reap the benefits of using information it collects, either for its own marketing purposes or by selling that information to a third party, without realizing possible losses from the misuse of such information. If the individual does not know who possesses his information, there is little he can do to protect his privacy. The relative ease and low cost of collecting personal identifiable information over the Internet magnify this concern.

The inability to monitor effectively the collection of personal identifiable information is coupled with a general lack of enforcement of self-regulatory principles. Furthermore, the inability to enforce self-regulatory principles may lead to overuse of personal information, and it could punish those that adhere to the principles by placing them at a competitive disadvantage against those who abuse the system.

256. See id. at 346 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (noting that poor oversight of self-regulatory efforts is due to a lack of a strong commitment and ability to enforce self-regulatory regimes); Swire, supra note 254, at 6 (stating that the costs of monitoring whether a company is complying with policies set under a self-regulatory regime are extremely high, making monitoring difficult, not to mention inefficient, because it is usually up to a customer to discover and report a company's noncompliance).

257. See Swire, supra note 254, at 6 (noting that the imperfect monitoring of company compliance results in customer ignorance of the full scale of the company's use of his information, rendering the customer unable to discipline the company effectively should it misuse such information).

258. See id. (stating that due to insufficient monitoring, individuals will not be able to know what a company knows about them and how that company uses the personal identifiable information that it does possess).

259. See supra notes 8-14 and accompanying text (discussing the ease and low cost of collecting personal identifiable information on the Internet). As databases containing personal identifiable information from various Web sites merge, it is unrealistic to think an individual will ever know who possesses their personal information. Cf. Riordan, supra note 21, at C9 (stating that a company has obtained a patent for a system that can gather personal information from thousands of Web sites, and then can turn that information into unique profiles). “Businesses want that [personal] information, and in the online world—where virtually every piece of data is for sale—they will probably get it.” Baig et al., supra note 1, at 84.

260. See OPTIONS PAPER, supra note 19, at 51 (arguing that a defect of U.S. data protection policy is that self-regulatory efforts are unenforceable because most self-regulatory codes are voluntary); see also Hearing on Issues in U.S.-European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy Before the House Comm. On Int'l Relations, 105th Cong. 68-69 (1998) [hereinafter Hearing on U.S.-EU Trade] (statement of Marc Rotenberg, Director, Electronic Privacy Information Center) [hereinafter Rotenberg Statement] (claiming that fair information practice principles, establishing the obligations of companies collecting personal identifiable information online, are often unenforceable in a self-regulatory regime due to weak and easily ignored safeguards).

261. See Henry H. Perritt, Jr., Regulatory Models for Protecting Privacy in the Inter-
Finally, when a company violates self-regulatory principles, the lack of a system of legal redress often deprives a harmed individual of a means of recourse.262 This situation may allow a company to violate self-regulatory policies without realizing any deterrent costs.263 If the company cannot be held accountable and the individual cannot seek a remedy when a breach of self-regulatory policies occur, then the incentive for a company to adhere to policy diminishes.264

A. Failure of Industry Initiatives to Adhere to Fair Information Practice Principles for the Online Collection of Personal Identifiable Information

Many of the private sector initiatives to protect online privacy have occurred through the articulation of guidelines issued by trade associations or industry groups for member companies.265 These guidelines often do not conform to stated fair information practice principles however, whether it is the principles articulated by the OECD, the IITF, the FTC, or the NTIA.266 The principle that is mentioned least in the industry-

---

262. See Mulligan & Goldman, supra note 254, at 66 (arguing that a lack of enforcement often leads “good” industry actors to suffer by the acts of “bad” actors due to diminished consumer confidence and a tarnished image in the industry). “[L]ike a cartel, a self-regulation framework tends to unravel because of ‘cheaters.’” Perritt, Jr., supra, at 107.

263. See Swire, supra note 254, at 6 (arguing that the lack of enforcement and legal redress for harmed individuals allows companies to benefit from the use of personal identifiable information without realizing significant costs).

264. See id. (arguing that when a company can receive the benefits of using information without incurring the costs of legal redress, the company will tend to overuse private information).

265. See supra Part II.D (discussing self-regulatory efforts of certain industries through industry-specific guidelines); see also FTC PRIVACY REPORT, supra note 9, at app. E (containing copies of nine industries’ online information practice guidelines and principles).

266. See Hearing on Privacy in Cyberspace, supra note 176, at 346 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (arguing that the current models for self-regulation do not incorporate the fair information principles); FTC PRIVACY REPORT, supra note 9 at 15-16 (studying industry-specific trade association and industry group online information guidelines and concluding that the “guidelines do not address all of the core fair information practice principles”). The FTC found that most industry guidelines encourage their members to provide individuals with some form of notice and choice online. See id. at 15. Many of the industry guidelines, however, do not provide guidance to their members as to how to provide an individual with access to the
specific guidelines is an enforcement mechanism to punish those who de-
viate from industry guidelines. In response to the failure of industry
guidelines to address enforcement, the FTC stated that "the absence of
enforcement mechanisms significantly weakens the effectiveness of in-
dustry-promulgated guidelines as a self-regulatory tool."

Although the TRUSTe and BBBOnLine Privacy programs appear to
be viable options for the protection of privacy online, many attorneys are
advising companies against posting privacy policies on their Web sites;
this fact is especially disheartening because these postings constitute the
very essence of these programs' framework. The fear of posting a pri-

vacy policy may continue in light of a recent settlement of an FTC com-
plaint against one of the most popular Web sites on the Internet, GeoCi-
ties. The complaint accused the Web site of engaging in deceptive
practices in connection with its collection and use of personal identifiable
information from its online customers. As a result of this complaint,
the FTC now believes that companies are being advised not to post pri-

vacy policies on their Web sites, thereby hindering the possibility that
Internet users will be provided with notice as to the companies' informa-
tion collection practices.

information that the company holds, and few address security issues. See id. at 16.

267. See FTC PRIVACY REPORT, supra note 9, at 16, 55 n.82 (noting that only the IRS
Principles condition further membership and information sharing on compliance with
them); see also Swire, supra note 254, at 8 (stating that industry codes designed to protect
privacy often provide for no legal enforcement, and the guidelines are only made available
to industry members and are not binding).

268. FTC PRIVACY REPORT, supra note 9, at 16.

269. See Eric Goldman, Esq., Drafting a Privacy Policy? Beware!, (visited Mar. 16,
1999) <http://www.ntia.doc.gov/ntiahome/privacy/files/9PK02!.HTM> (explaining that
companies can expose themselves to an enormous amount of liability by posting a privacy
policy); Esther Dyson, Privacy Protection: Time to Think and Act Locally and Globally,
that lawyers are advising businesses that making promises to consumers about the protec-
tion of their personal identifiable information will only expose those companies to liabil-
ity).

270. See Federal Trade Commission, In the Matter of GeoCities: Complaint (visited

271. See id. The complaint alleges that GeoCities falsely represented itself by posting
a privacy policy that stated that: (1) personal identifiable information that it collects
through a membership form was used only to provide members with specific advertising
offers, when in fact the information was sold to third parties, (2) "optional information"
collected on the application form would not be disclosed to third parties, when in fact it
was, and (3) it collects and maintains children's personal identifiable information obtained
through online contest entry forms, when in fact the contests were run by a third party
who actually collected and stored children's information. See id. at ¶¶ 9-20.

272. See Joel Brinkley, F.T.C. Surfs the Web and Gears Up to Demand Privacy Protec-
tion, N.Y. TIMES, Sept. 21, 1998, at C1 (citing FTC officials' conclusions that the consensus
among businesses is that if no privacy policy is posted then the FTC will not have authority
There also may be a conflict of interest problem when a program, such as TRUSTe or BBBOnLine, is faced with disciplining one of its corporate sponsors. This issue emerged when TRUSTe decided not to pursue an audit of Microsoft's privacy practices following a complaint about the personal identifying number on Microsoft products. Microsoft is a corporate sponsor of TRUSTe and has contributed $100,000 to the TRUSTe program. TRUSTe's decision not to pursue Microsoft's information collection practices adds currency to the argument "that these seals don't deliver the real privacy protection that people want and deserve, and self-regulation is sham regulation."

B. The Lack of a Federal Regulatory Authority to Protect Privacy

A possible reason that industries have failed to address fully fair information practices is that four different sources, three of them United States Government agencies, have established fair information practice principles for the collection of personal information online. In the United States, the FTC, IITF, and NTIA all have released reports describing fair information practice principles for the collection of personal identifiable information online. The OECD, however, concluded that the fair information practice principles articulated in its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data should apply to the online environment. Although each source pro-

---

273. See Jeri Clausing, On-Line Privacy Group Decides Not to Pursue Microsoft Case, N.Y. TIMES, Mar. 23, 1999, at C5 (discussing a decision by TRUSTe not to conduct audit proceedings against Microsoft, a leading corporate sponsor).

274. See id. (reporting that Microsoft included an identification number in its Windows98 operating system that collected data from users without their knowledge). TRUSTe declined to reprimand Microsoft because it claimed it did not find violations of the program's mandates on Microsoft's Web site. See id.

275. See id.

276. Id. (quoting Jason Catlett, president of Junkbusters Corporation).

277. See supra Part II.A (discussing the development of fair information privacy practice principles by the OECD, IITF, FTC, and NTIA).

278. See generally Elements of Effective Self Regulation for the Protection of Privacy, 63 Fed. Reg. 30,729 (1998) (publishing the NTIA's principles); FTC PRIVACY REPORT, supra note 9; IITF PRINCIPLES, supra note 125.

279. See OECD INTERNET PRIVACY, supra note 28, at 4 (concluding that the OECD
vides similar principles, the failure to adopt any single approach as a national policy leads to confusion among those who must implement the principles in order to protect online privacy.280

Furthermore, the Federal Government has not granted or delegated the authority to protect privacy to an existing Federal agency as its sole objective or mission.281 Neither the IITF, the FTC, nor the NTIA commit all of their resources to protecting individual privacy on the Internet; as a result, privacy must compete with other initiatives and responsibilities of these Federal agencies.282

C. Federal Trade Commission Survey of Commercial Web Sites

Thus far, this discussion has focused on general problems facing self-regulatory regimes; however, in March 1998, the FTC conducted a survey of 1,402 commercial Web sites to determine if self-regulation was having a practical effect on the protection of privacy online.283 The FTC found that a significant amount of personal identifiable information was being

---

280. See Hearing on Privacy in Cyberspace, supra note 176, at 345-46 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (noting that the variety of fair information practice principles articulated tend to confuse both the business community and the public); Hearing on U.S.-EU Trade, supra note 260, at 69 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (stating that "the absence of a clear privacy standard in the US means that less favorable standards are being developed").

281. See OPTIONS PAPER, supra note 19, at 58 (observing that the United States does not have a centralized entity to drive development of a Federal data privacy policy or to oversee the privacy initiatives currently underway).

282. See id. at 51. Not only does this fact confuse American businesses, but it also means that the United States does not have an identifiable representative to discuss privacy concerns with international trading partners. See id. at 50-51.

283. See FTC PRIVACY REPORT, supra note 9, at 19 (providing an overview of the survey). The FTC broke the survey down into six samples: (1) the Comprehensive Sample of 674 commercial sites in the United States that were "likely to be of interest to consumers"; (2) the Health Sample of 137 sites considered to be a part of the health sector; (3) the Retail Sample consisting of 142 sites; (4) the Financial Sample of 125 sites; (5) the Children's Sample of 212 sites; and (6) the Most Popular Sample, surveying the 111 most popular Web sites. See id. at 19. The notes in this section also consider a June 1999 privacy policy survey that serves as a progress report to the FTC PRIVACY REPORT. See MARY H. CULNAN, GEORGETOWN INTERNET PRIVACY POLICY SURVEY: REPORT TO THE FEDERAL TRADE COMMISSION 6 (1999) (studying 361 Web sites drawn from a sample of the 7500 top universal resource locators [Web site addresses] "ranked by audience during January 1999"). In studying the "extent to which commercial Web sites have posted privacy disclosures based on fair information practices," the Georgetown Internet Privacy Policy Survey addressed three questions: (1) what type of personal information, if any, does the Web site collect; (2) does the Web site post a privacy disclosure; and (3) does the privacy disclosure encompass fair information practice principles? See id. at 10.
collected from individuals online. Though the vast majority of Web sites collected personal identifiable information, few of the sites disclosed to consumers their information collection practices.

From these findings the FTC concluded that there is a need to implement fair information practice principles to protect online privacy. The FTC noted that the low cost and efficient means of collecting personal identifiable information on the Internet creates a more complex problem for the protection of individual privacy than did the traditional means of collection. Recognizing that the majority of online businesses do not provide the fundamental fair principles of notice and awareness, the FTC concluded that, despite the agency’s three-year commitment to support self-regulation, it “has not seen an effective self-regulatory system emerge.”

284. See FTC PRIVACY REPORT, supra note 9, at 23 (finding that 92% of Web sites in the Comprehensive Sample of 674 sites collected personal identifiable information). At least 87% of the Web sites in each FTC sample, excluding the Children’s sample, collected personal information from consumers visiting their Web sites. See id. at 24. The Georgetown Internet Privacy Policy Survey found that 92.8% of the Web sites surveyed collected at least one type of personal identifying information. See CULNAN, supra note 283, at 10. That survey defines “personal identifying information” as “information that can be used to identify a consumer such as a name or e-mail address,” as opposed to “demographic information” which “by itself cannot be used to identify a consumer.” See id. The Georgetown Internet Privacy Policy Survey found that 81.2% of those Web sites surveyed collected the visitor’s name, and 90.9% collected the visitor’s electronic mail address. See id. at 11.

285. See FTC PRIVACY REPORT, supra note 9, at 27-29 (finding that only 14% of the Web sites in the Comprehensive Sample disclosed their information collection practices to individuals visiting their sites). The sample of the most popular sites, however, found that 71% disclose their information collection practices, demonstrating that providing notice is possible; however, it is not being done on a widespread basis. See id. at 28. But see CULNAN, supra note 283, at 13 (finding that 65.9% of the Web sites surveyed had at least one privacy disclosure). Notably, the Web sites from the Most Popular Sample were on notice by press reports and public statements that the FTC was going to survey their sites; despite this notice, over one quarter of the sites chose not to create privacy policies. See FTC PRIVACY REPORT, supra note 9, at 28-29.

286. See FTC PRIVACY REPORT, supra note 9, at 40 (concluding that the practices of the Web sites surveyed show a “real need” to implement basic privacy protections described in the fair information practices).

287. See id. (stating that the efficiencies of the Internet, allowing for an easy and low cost means of collecting data, demand that the United States take control of this problem).

288. See id. at 41. The Georgetown Internet Privacy Policy Survey demonstrates the lack of an implementation of fair information practice principles in Web site privacy disclosures, calling into question whether these Web sites are practicing the principles articulated by such agencies as the FTC and the Department of Commerce. See CULNAN, supra note 283, at 14 (researching the extent to which posted privacy disclosures “by Web sites are based on fair information practices”). The Georgetown Internet Privacy Policy Survey searched the privacy policies of the Web sites “to determine if they included notice, choice, access or security,” and whether contact information was provided to the visitor in
**D. Self-Regulation and the EU Data Privacy Directive**

Article Twenty-five of the EU Data Privacy Directive, which came into force in late October of 1998, only allows the transfer of personal information to third countries—non-EU countries—that provide “adequate” privacy protection.\(^{289}\) The EU considers “the degree to which its rules can be enforced” a vital criterion in assessing whether a self-regulatory policy will be deemed “adequate” to satisfy Article Twenty-five.\(^{290}\) In evaluating self-regulation as an adequate means of protection, the EU considers whether the content of a “self-regulatory code” contains certain core principles.\(^{291}\) The EU also evaluates the effectiveness of self-regulation to achieve “a good level of general compliance[,] . . . support and help to individual data subjects [.and] appropriate redress.”\(^{292}\)

Currently the U.S. industry guidelines to protect privacy in the online environment are devoid of the core principles the EU requires.\(^{293}\) The

\(^{289}\) See EU Data Privacy Directive, supra note 31, art. 25, at 45-46 (establishing principles for the transfer of personal data from EU member states to non-EU countries).

\(^{290}\) See Working Party, supra note 190 (stating the EU’s concern regarding the ability of self-regulatory industry groups to impose sanctions for noncompliance with the code).

\(^{291}\) See id. at Annex (suggesting that the content of self-regulatory industry codes include a purpose principle, a data quality and proportionality principle, a transparency principle, a security principle, an access, rectification and opposition principle, and restrictions on transfers to non-EU countries).

\(^{292}\) Id. (evaluating self-regulation). According to the EU, a good level of compliance with an industry code “is likely to depend on the degree of awareness of the code’s existence,” on the steps taken to provide consumers with notice of the industry code and practices, and most importantly, “on the nature and enforcement of the sanction in cases of non-compliance.” Id. (evaluating the effectiveness of a self-regulatory instrument). The EU also recommends that an effective system provide institutional support to an individual faced with a problem regarding his personal data. See id. It suggests that an appropriate remedy, including damages and correction of data, be available to the harmed individual should a self-regulatory code be breached. See id.

\(^{293}\) See Hearing on Privacy in Cyberspace, supra note 176, at 346 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (discussing the failure of industry guidelines in the United States to provide many of the well-established fair information practice principles, specifically enforcement and legal redress mecha-
FTC survey indicates that general compliance with fair information practice principles is seriously lacking. In addition, the U.S. policy of self-regulation for the protection of privacy online fails to provide the appropriate redress sought by the EU. As a result of the failure to meet the requirement to provide adequate privacy protection, there is at least some risk that communications between Europeans and Americans may be shut down due to the ineffectiveness of self-regulation.

IV. TIME TO REVAMP THE SYSTEM

The main concern of online users is the failure of self-regulators to protect the privacy of the users' personal identifiable information. To put this worry to rest, the United States should pass legislation that will ensure that individual privacy is protected online. By formally adopting one set of privacy principles and establishing a regulatory body responsible for the monitoring and enforcement of such principles, consumer confidence in the Internet will grow, and the full benefits of this...
new and exciting medium can flourish. This is not to say that the United States should abandon self-regulation; rather, it should help promote programs such as TRUSTe and BBBOnLine while, at the same time, providing online users with a sense of security through effective legislation.

A. Legislation is Needed to Protect Privacy Online

Under the current self-regulatory system in the United States, fair information practice principles may be recognized, but they are not followed consistently. Therefore, the United States should adopt a single set of fair information practice principles and mandate that companies collecting information online adhere to these practices on their Web sites. Specifically, the United States should adopt the FTC privacy principles, as they exemplify a common ground of information privacy principles.

To adopt a set of fair information practice principles, the United States has two options available. The first option is to follow Canada’s lead and adopt a “model code” for self-regulation. This model delineates a set

---

299. See OPTIONS PAPER, supra note 19, at 53 (discussing that one option that Congress may consider to protect privacy over the Internet is the establishment of omnibus privacy legislation adopting a set of privacy principles, coupled with agency specific regulation); see also Hearing on Privacy in Cyberspace, supra note 176, at 314 (statement of Hon. Robert Pitofsky, Chairman, Federal Trade Commission) (stating that “one of the principal reasons why the Internet is not developing as a commercial marketplace is that people are so concerned about the way in which personal information will be used”).


301. See generally Elements of Effective Self-Regulation for the Protection of Privacy, 63 Fed. Reg. 30729 (1998) (stating the NTIA’s principles that are part of the elements of an effective self-regulatory privacy regime); FTC PRIVACY REPORT, supra note 9, at 7-11 (articulating privacy principles for the collection and use of personal identifiable information derived from a collection of principles stated in the past); IITF PRINCIPLES, supra note 125 (establishing fair information practice principles for the protection of personal identifiable information in the online environment). Cf. FTC PRIVACY REPORT, supra note 9, at 19-43 (discussing the failure of industry guidelines and commercial Web sites to adhere to traditional fair information practice principles).

302. See Hearing on Privacy in Cyberspace, supra note 176, at 349 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (proposing that all Web sites that collect and use personal identifiable information be required to comply with a uniform national policy of enforceable fair information practices).

303. See FTC PRIVACY REPORT, supra note 9, at 7, 48 n.28 (describing the FTC principles as the common principles of previous reports, guidelines, and model codes concerning fair information practice principles).

304. See CSA MODEL CODE, supra note 34 (establishing a voluntary national standard
Protecting Privacy Over the Internet

of privacy practice principles and requires companies to implement the principles as a whole. This method would solve the problem evidenced by the FTC Report: companies adhering to only a few of the accepted privacy principles.

Alternatively, and preferably, Congress can adopt legislation codifying a set of fair information practice principles for the collection of personal identifiable information online. Online consumers favor legislation in this area, and legislation may be beneficial to online companies who currently adhere to fair information practice principles. The conversion of the FTC fair information practice principles into law would not burden online companies because they are phrased in broad terms.

B. The United States Should Establish a Privacy Regulatory Authority

Commentators have stated many times that an enforcement mechanism is necessary to ensure companies' compliance with fair information practices. Therefore, the federal government either should grant regulatory authority to an existing federal agency or create a new privacy

of privacy principles in the collection and use of personal identifiable information to further self-regulatory regimes).

See id. § 3.1 (requiring that the ten principles described in the CSA Model Code be adopted as a whole in order to standardize fair information practices of all Canadian companies adopting the code); see also Bennett, supra note 33, at 158 (stressing that organizations cannot pick and choose which principles they wish to follow).

See supra Part III.A (discussing the failure of industry guidelines and commercial Web sites to follow all of the FTC's stated fair information practice principles).

See supra note 176, at 308 (statement of Hon. Robert Pitofsky, Chairman, Federal Trade Commission) (proposing that privacy legislation set out basic standards of practice governing the collection and use of personal identifiable information online).

See supra notes 261, 298 and accompanying text (describing consumer survey results pertaining to feelings of legislation to protect privacy over the Internet); see also supra note 263 and accompanying text (discussing the competitive disadvantage that good actors face when they adhere to privacy policies and others do not due to lack of enforcement).

See Hearing on Privacy in Cyberspace, supra note 176, at 308 (statement of Hon. Robert Pitofsky, Chairman, Federal Trade Commission) (suggesting that any legislation defining fair information practices should be broad to allow for flexibility due to the fact that implementation will vary by industry). The legislation could also include a safe harbor for those companies that comply with the fair information practice principles through industry self-regulatory regimes. See id. at 309.

See supra notes 260-63 and accompanying text (discussing the effects that a failure to provide enforcement procedures may have on the protection of privacy online); see also FTC PRIVACY REPORT, supra note 9, at 10 (stating that "[t]o be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress)").
agency under the Administrative Procedure Act,\textsuperscript{311} to monitor, enforce, and adjudicate consumer claims alleging an invasion of privacy.\textsuperscript{312} The FTC is best suited to administer these tasks because it has been working on the issue of online privacy for over three years.\textsuperscript{313} Currently, however, the FTC may not have the resources necessary to handle this task effectively on a full-time basis.\textsuperscript{314}

For this reason, Congress should create a new federal agency to deal with online privacy issues.\textsuperscript{315} A federal agency devoted to privacy protection online can monitor companies on the Internet as well as levy sanctions for noncompliance with fair information practice principles.\textsuperscript{316} This measure would establish the monitoring, enforcement, and legal redress mechanism necessary for effective regulation and also, coupled with legislation establishing fair information principles, would satisfy the EU Data Privacy Directive, thereby preventing any interruption of data transfer.\textsuperscript{317} Moreover, a federal privacy agency could fill a current void left by the United States in international relations and negotiations of privacy rights, finally giving the United States a single entity to which both domestic companies and foreign governments can look in address-


\textsuperscript{312} See Hearing on Privacy in Cyberspace, supra note 176, at 308 (statement of Hon. Robert Pitofsky, Chairman, Federal Trade Commission) (arguing for the establishment of a new privacy agency to compliment legislation by providing additional recommendations for the protection of online privacy); OPTIONS PAPER, supra note 19, at 58-61 (stating that the government could set up a new privacy agency with “quasi-legislative” and “quasi-judicial” authority or give an existing agency additional authority).

\textsuperscript{313} See Hearing on Privacy in Cyberspace, supra note 176, at 350 (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology) (recommending that the FTC be granted authority to establish a backbone for the protection of privacy of personal identifiable information, due to the FTC’s accumulated knowledge and expertise stemming from addressing online privacy for over three years).

\textsuperscript{314} See OPTIONS PAPER, supra note 19, at 60-61 (describing the possible drawbacks of granting an existing federal agency with additional authority over privacy regulation). Placing privacy regulation and adjudication authority in the hands of the FTC would mean that privacy would have to compete with other purposes and responsibilities of the FTC, which may lessen the effectiveness of the privacy entity. See id.

\textsuperscript{315} See Jerry Berman and Deirdre Mulligan, CDT Submits These Comments on the Draft “Options for Promoting Privacy on the National Information Infrastructure” (visited Nov. 2, 1998) <http://www.cdt.org/privacy/intia.html> (recommending that an agency be established to provide the “scope, expertise, and authority to guide public policy”).

\textsuperscript{316} See OPTIONS PAPER, supra note 19, at 59 (explaining that regulatory agencies can control private conduct by promulgating and implementing rules and regulations, as well as imposing sanctions on violators of those rules and regulations).

\textsuperscript{317} See supra Parts II.B, III.D and accompanying text (discussing the requirements of the EU Data Privacy Directive and how the EU will interpret “adequate” privacy protection).
ing privacy issues. 318

C. The United States Should Continue to Promote Effective Self-
Regulatory Projects and Technologies

The passing of broad legislation and the granting of regulatory author-
ity to an independent Federal agency should not spell the end for indus-
try self-regulation. 319 The Government should promote programs such as
TRUSTe and BBBOnLine, and should encourage the advent of new
technology that one day may render concerns over the privacy of per-
sonal identifiable information on the Internet obsolete. 320 As for now,
steps must be taken to solidify U.S. policy and cure the ills of self-
regulation; however, because of the Internet’s size and growth, continued
self-regulated industries should work with the Government to promote
the privacy rights of individuals online.

V. CONCLUSION

Self-regulation has had over three years to catch on in the online in-
dustry, yet to date it has failed. The privacy of personal identifiable in-
formation should not be compromised any longer. With more than sev-
enty million of its citizens currently online, the United States must move
to the forefront of protection instead of taking a backseat to Europe and
Canada. If the Internet age is truly the wave of the future, consumer
confidence will have to lead the way. As of now, that confidence is
lacking because an effective regulatory regime is lacking. If consumers
hold true to their word, creating laws to protect privacy over the Internet
should lead to the further growth of the Internet and electronic com-
merce. The Honorable Robert Pitofsky, Chairman of the FTC recog-
nized that too few “appreciate that one of the principal reasons why the
Internet is not developing as a commercial marketplace is that people are
so concerned about the way in which personal information will be
used.” 321 It is time to come to this realization, and for the United States
Government to protect its citizens’ “right to be let alone.”

318. See OPTIONS PAPER, supra note 19, at 63 (claiming that currently, members of
the international community have a difficult time identifying a single point of contact on
privacy issues in the United States).

319. See Budnitz, supra note 300, at 884-85 (noting that continued self-regulation can
compliment privacy legislation, giving consumers even more confidence).

320. See supra Part II.E (discussing the benefits of the TRUSTe program and the
BBBOnline program).

321. See Hearing on Privacy in Cyberspace, supra note 176, at 314 (statement of Hon.
Robert Pitofsky, Chairman, Federal Trade Commission).