4-1-2003

The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond

Paige Norian

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

Recommended Citation
Available at: http://scholarship.law.edu/lawreview/vol52/iss3/8

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 administrator of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.
THE STRUGGLE TO KEEP PERSONAL DATA PERSONAL: ATTEMPTS TO REFORM ONLINE PRIVACY AND HOW CONGRESS SHOULD RESPOND

Paige Norian

Millions of Americans use the Internet for various activities everyday. We make travel plans, purchase gifts, pay bills, check our credit card and bank balances, and send e-mail messages to friends and co-workers. But are we so naïve as to think that our online activities are kept private?

Before the September 11th terrorist attacks, privacy was the leading technology issue facing Congress. Advances in information technology outpaced existing laws protecting personal privacy. Congress recognized this inadequacy and began to focus its efforts on online privacy regulation. This effort resulted in a combination of legislation and promotion of industry self-regulation, both aimed to protect personal data and privacy on the Internet.

---

1. Patrick Thibodeau, Congress Eyes Privacy Issues, COMPUTERWORLD (Sept. 25, 2002), available at http://story.news.yahoo.com/news (last visited Oct. 6, 2002). For legal purposes, there are at least four different definitions of privacy: 
   “(1) [i]ntrusion upon the [individual’s] seclusion or solitude, or into his private affairs; (2) [p]ublic disclosure of embarrassing private facts about the [individual]; (3) [p]ublicity which places the [individual] in a false light in the public eye; [and] (4) [a]ppropriation, for another person’s advantage, of the individual’s name or likeness.” William Prosser, Privacy, 48 CAL. L. REV. 383, 389 (1960).

2. See Thibodeau, supra note 1. The Advanced Research Projects Agency (ARPA) developed the Internet in 1969 to allow government computers in the United States to exchange information during wartime without interruption. Michelle Z. Hall, Comment, Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web, 18 N.Y.L. SCH. J. HUM. RTS. 609, 613 (2002). Later, universities used the Internet to exchange research. Id. at 613. The “Internet is a publicly used global system comprising a complex series of interconnected computer networks that communicate via telephone lines, fiber optics, copper wires, satellite transmissions, and other dedicated data connections.” Id. at 613.


This piecemeal approach has led to insufficient reforms in the area of online privacy. Many online companies attempt to address public concerns by developing privacy policies, hiring privacy officials, and supporting third-party accreditation services. Problems arise when companies either change or fail to follow their privacy policies without notifying consumers. In addition, some companies post privacy policies that are difficult to understand, misleading, or contradictory. Frequently, online companies acquire information from customers for their own purposes and then sell that information to other companies without customers' knowledge or consent. In one extreme case, a company provided assurances of protection, but when it ran into financial troubles, it sold its customers' data to the highest bidder. While some progress has been made, serious problems remain, furthering the need for effective federal reform.

In the aftermath of the terrorist attacks, Congress understandably focused on enhancing security. As law enforcement agencies began employing commercial data services to capture potential terrorists, Americans raised the concern that government counterterrorism investigations were greatly diminishing individual privacy rights. In

7. See id.
8. Id.
10. See id.
response, several privacy bills aimed at limiting the collection or use of customer information obtained online were introduced in the 107th Congress. Among the many pending bills, congressional attention is currently focused on S. 2201, the Online Personal Privacy Act (OPPA) of 2002, and H.R. 4678, the Consumer Privacy Protection Act (CPPA) of 2002. Although both bills seek to regulate the collection, use, and dissemination of personal information online, significant differences between the bills require close analysis to determine which will be the most effective in protection of online privacy.

This Comment examines the debate over data protection in the midst of technological innovations, specifically the Internet. First, this Comment traces the development of the fundamental right to privacy through constitutional interpretation and judicial decisions. Next, it discusses existing privacy laws that regulate the collection and use of personal information in specific industries. In addition, this Comment discusses industry self-regulation practices. Then, it analyzes the gaps in privacy protection left by the existing laws. It also evaluates two current proposals for a comprehensive online privacy law, the OPPA and CPPA, for their strengths and weaknesses. Finally, this Comment details how both proposals fill the gaps left by past legislation and concludes that

PATRIOT Act by "lower[ing] the threshold for when ISPs may divulge the content of communications, and to whom." MARCIA S. SMITH, CONGRESSIONAL RESEARCH SERVICE, INTERNET PRIVACY: OVERVIEW AND PENDING LEGISLATION 6 (Aug. 28, 2002). Ms. Smith further reports that "under H.R. 3482, the ISP would need a "good faith" belief (instead of a "reasonable" belief) that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury." Id.


Congress should pass the OPPA because it provides consumers with stronger privacy protections for personal information.

I. DEVELOPMENT OF ONLINE PRIVACY AND CONGRESSIONAL EFFORTS TO REGULATE

A. Foundations of Privacy

The United States Constitution establishes the basis for a national dialogue regarding institutional relationships and fundamental values. Although the U.S. Constitution does not explicitly mention the right to privacy, according to one commentator, the Bill of Rights prohibits states from "interfering in the exercise of certain activities," "carrying out certain kinds of collection," and "utilizing personal information." The Fourth Amendment, for example, protects individuals from unreasonable searches and seizures. In addition, the First Amendment protects an individual's associational rights. Several Supreme Court

17. Id. at 566-67.
18. U.S. CONST amend. IV. The Fourth Amendment states:
   The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
Id. In Katz v. United States, the Supreme Court held that the unreasonable searches and seizures provision of the Fourth Amendment "protects people, not places." 389 U.S. 347, 357 (1967). The Katz opinion states that what a person knowingly exposes to the public is not subject to Fourth Amendment protection, but what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Id. at 351-52. Justice Harlan's concurrence presents a two-part test for determining an individual's expectation of privacy. Id. at 361. First, the individual must exhibit a subjective expectation of privacy, and second, "the expectation must be one that society is prepared to recognize as 'reasonable.'" Id.
19. U.S. CONST. amend. I. ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.") In NAACP v. Alabama, the Supreme Court held that the right to associate freely could be limited if the restriction served a compelling governmental interest unrelated to the suppression of ideas and more narrowly tailored means were unavailable to further the state interest. See NAACP v. Alabama 357 U.S. 449, 464-66 (1958). The issue in this case was whether the state could enforce a law that required out-of-state corporations to meet certain licensing qualifications. See id. at 451. This law enabled the Attorney General of Alabama to compel production of a large number of the NAACP's records, including lists of members' names. See id. at 451-52. The Supreme Court concluded that if the state had access to the organization's membership list, it would adversely affect the NAACP's ability to carry out its mission. Id. at 462. Thus, the Court concluded that Alabama's data collection scheme infringed
decisions have shaped current law regarding privacy by elaborating on the protections provided in the First and Fourth Amendments.20

1. Supreme Court Recognition of a Right to Privacy

In an influential Harvard Law Review article, Samuel Warren and Louis Brandeis asserted what has become the basic principle of American privacy law: the “right to be let alone.”21 The article addressed invasions of personal privacy due to technological advancements of the late nineteenth century.22 Warren and Brandeis urged the courts to recognize a person’s right to be free from unwarranted intrusions into personal affairs.23 They also argued that “the privacy of the individual should receive the added protection of the criminal law.”24 This article served as the foundation for evolving case law over the years and remains a guideline in current privacy litigation.25

Justice Brandeis again declared the meaning of the right to privacy to be “the right to be let alone” many years later in his dissenting opinion in Olmstead v. United States.26 He characterized “the right to be let alone” upon its members’ First Amendment right of association and was, therefore, unconstitutional. See id. at 466. The Court protected the “freedom to associate and privacy in one’s associations,” noting that freedom of association was a peripheral First Amendment right. Id. at 462.

20. See Gibson v. Florida Legislative Investigative Comm., 372 U.S. 539, 557-58 (1963) (reversing the contempt judgment for not disclosing information contained in the organization’s membership list); see also Bates v. Little Rock, 361 U.S. 516, 527 (1960) (reversing convictions for the violation of a municipal occupational license tax compelling disclosure and publication of membership lists); NAACP, 357 U.S. at 466 (reversing judgment of contempt for refusing to disclose membership lists).

21. Samuel Warren & Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890). In this article, Warren and Brandeis “consider[ed] whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.” Id. at 197. According to the authors, “the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing . . . so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone.” Id. at 205.

22. See id. at 195-96; see also Hall, supra note 2, at 611-12 (noting that Warren and Brandeis’ article was written in response to the invention of mass printing and portable cameras and further noting that gossip in the press offended the authors).

23. See Warren & Brandeis, supra note 21, at 215. Warren and Brandeis believed: “It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented.” Id. at 215.

24. Id. at 219. The authors stated, “It is not for injury to the individual’s character that redress or prevention is sought, but for injury to the right of privacy.” Id. at 218.


26. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). The issue in this case was whether federal agents could tap telephone wires without violating the defendant’s Fourth and Fifth Amendment rights. Id. at 455. The Supreme Court ruled that no warrant was
as "the right most valued by civilized men." In addition, Justice Brandeis stated that "[t]o protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual . . . must be deemed a violation of the Fourth Amendment." Modern developments in technology, such as the electronic storing of personal data, turned the prophetic fears voiced by Justice Brandeis into a reality.

Although the right to privacy is not explicit in the Constitution, the Supreme Court recognized a fundamental constitutional right to privacy under the "penumbra" theory. In Griswold v. Connecticut, the Court held that certain rights, such as the right to privacy, were found in the shadows of the Bill of Rights. Justice Douglas stated that specific guarantees in the Bill of Rights have "penumbras, formed by emanations from those guarantees that help give them life and substance." He further stated that "various guarantees . . . create zones of privacy." In decisions following Griswold, the Court interpreted the Bill of Rights as creating, through its penumbras, "a right of personal privacy, or a

necessary for federal agents to tap telephone wires because it did not amount to a search or seizure within the meaning of the Fourth Amendment. Id. at 464-65. The Court held that the Fourth Amendment only protects against physical invasions by law enforcement officers. Id.

27. Id. at 478.

28. Id.

29. See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193 (1998) (noting that the potential for wide-ranging surveillance of cyberspace activities presents a significant threat to information privacy). Cyberspace refers to the "web of consumer electronics, computers, and communication networks that interconnects the world." Id. at 1195. Furthermore, the "revolution in our communications infrastructure -- in particular, the explosive growth of the Internet -- has fundamentally transformed how we create, acquire, disseminate, and use information." Id. For the past thirty years, "many have warned about the privacy dangers posed specifically by the computer." Id. at 1199.

30. Griswold v. Connecticut, 381 U.S. 479, 484 (1965); see also Mapp v. Ohio, 367 U.S. 643, 656 (1961) (noting that the Fourth Amendment creates a "right to privacy, no less important than any other right carefully and particularly reserved to the people").

31. 381 U.S. 479 (1965).

32. Id. at 484. In Griswold v. Connecticut, Appellant Griswold, Executive Director of the Planned Parenthood League of Connecticut, and Appellant Buxton, Medical Director for the League, were arrested for violating state statutes that made it unlawful to assist others in preventing conception. Id. at 480. Appellants provided married persons with advice and instruction regarding the use of contraceptive devices. Id. The Court found the statute unconstitutional, thereby recognizing a right to marital privacy. See id. at 485-86.

33. Id. at 484.

34. Id. The Court explained that "the right of association contained in the penumbra of the First Amendment" is one particular zone of privacy. Id. Similarly, "[t]he Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment." Id.
guarantee [that] certain areas or zones of privacy [do] exist under the Constitution.\textsuperscript{35} Despite this judiciously recognized right to privacy, the Supreme Court has yet to extend this right to personal information.\textsuperscript{36}

2. Expanding Privacy Rights to the Internet

The development and increasing use of the Internet has sparked debate regarding an individual’s privacy rights online.\textsuperscript{37} Privacy advocates suggest that “the right to be let alone” should include a right to “information privacy” for online transactions requesting personally identifiable information.\textsuperscript{38} The term “information privacy” is described as the “desire of individuals to limit the kinds of information that others know about them.”\textsuperscript{39} Maintaining information privacy is difficult because both the individual and the online information collector claim control of the personal data.\textsuperscript{40}

The Internet provides companies with the ability to collect information about their users and to distribute that information to others.\textsuperscript{41} Through

\textsuperscript{35.} Roe v. Wade, 410 U.S. 113, 152-54 (1973) (holding that the right to privacy is broad enough to encompass a woman’s decision whether to terminate her pregnancy); see also Paul v. Davis, 424 U.S. 693, 712-13 (1976) (holding that the Constitution protects a right of privacy from governmental intrusions regarding intimate personal decisions concerning matters relating to marriage, procreation, contraception, family relationships, child rearing, and education).

\textsuperscript{36.} See Kramer, supra note 4, at 401-02 (noting that in the United States, exploiting personal information for business-related matters is a common domestic activity).

\textsuperscript{37.} See Gina Marie Stevens, Congressional Research Service, Online Privacy Protection: Issues and Developments 5 (Jan. 11, 2001).

\textsuperscript{38.} Id. All Internet activity, even simply browsing a Web page, involves a “transaction’ between an individual and a transacting party.” Kang, supra note 29, at 1246. While some of these transactions involve standard e-commerce, other transactions involve more sensitive exchanges. See id. at 1246. For example, an e-mail correspondence between a patient and doctor contains confidential medical information that should be kept privileged. See id. Personal information is generated from these interactions. See id. Thus, the transacting party and the transaction facilitators become potential information collectors. See id.

\textsuperscript{39.} Steven C. Carlson & Ernest D. Miller, Public Data and Personal Privacy, 16 Computer & High Tech. L.J. 83, 87 (1999) (noting that information privacy is one kind of privacy interest that individuals possess). Information privacy also includes “disclosures of personal data that . . . reveal information that would not otherwise be known.” Id. at 87. Other privacy interests important to individuals include an “interest in personal security and safety” and “due process interests in the proper handling of their data.” Id. at 86-87.

\textsuperscript{40.} See Kang, supra note 29, at 1246. Individuals may not want information collectors to share their personal data either because they fear that the information will be misused or because they want to avoid embarrassment due to the sensitive nature of the information. See id. Information collectors, however, seek control of the information for uses such as database marketing. See id.

\textsuperscript{41.} See Hall, supra note 2, at 613-16. Personal information about Internet users is becoming easy to collect due to software implementations known as “cookies.” Id. at 614.
a process known as "personalization," online companies generate personalized Web pages for customers based on the demographic data they provide. Companies also obtain demographic data by monitoring browsing and buying patterns of customers who visit their Web sites. Such practices often frustrate the public's desire to maintain information privacy.

The Supreme Court developed the framework for a constitutional right to information privacy in Whalen v. Roe. This case concerned a state statute that established a centralized computer file containing names and addresses of all persons who obtained certain drugs pursuant to a doctor's prescription. Although the Supreme Court upheld the state statute, it identified two interests affected by this governmental gathering of information. The first interest was "the individual interest in avoiding disclosure of personal matters." The second was "the interest in independence in making certain kinds of important decisions." In effect, Whalen established that the right of individuals to

"Cookies" enable Web sites to identify users each time the user visits the site. Specifically, cookies have the ability to record a user's "preferences" when visiting a Web site and then store those preferences on the user's hard drive. This cookie is later transmitted back to the Web site, identifying which computer is requesting information along with the particular areas already seen from that Web site. Frequently, the information is "exchanged without the user's knowledge or consent." Internet providers argue that cookies are not a privacy violation because they "cannot be placed on a computer without the user's 'permission'" and because "a cookie is required to allow the accessed content provider instant retrieval of what information a user has previously sought." Privacy advocates argue, however, that most users are unaware they are permitting cookie storage. Appellees argued that the statute impaired these interests. The Court acknowledged this concern by stating that "the mere existence in a readily available form of the information about patients' use of [certain] drugs creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations."
control access to their information is not absolute. Following Whalen, courts have identified several factors to evaluate challenged practices and statutes concerning data processing, including: the nature of the statute requiring information collection; the potential harm through future disclosures; and the state's need to access the information. Additionally, courts consider the "adequacy of the safeguards to prevent unauthorized disclosures."

Privacy advocates support legal recognition of a right to informational privacy for online transactions. Although the Constitution provides limited protection for the privacy of personal information, this protection applies only to government intrusions. Congress has not addressed the disposition of personally identifiable information in a comprehensive manner; instead, it chose a piecemeal approach. Legislators have generally passed privacy laws only in response to a specific event or concern, without careful consideration of preexisting laws. The resulting patchwork of laws left significant gaps in online privacy.

---

50. See id. at 597-98.
52. Id. at 576-77.
53. See STEVENS, supra note 37, at 5.
54. Id. In effect, these protections are inadequate because many threats to the privacy of personal data occur in the private sector. Id.
55. Id. at 7. Congress has enacted a number of industry-specific federal laws to protect the privacy of certain personal information. See id. at 7-9. These laws include regulation of the use and disclosure of personal information from state motor vehicle records as well as personal information collected in connection with video rentals. See Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2000); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000). In addition, limitations are placed on the disclosure of cable television subscriber information for mail solicitation purposes. See Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000). None of these laws, however, address privacy in the context of online personal information. See STEVENS, supra note 37, at 7.
56. See, e.g., Privacy and Internet Communication, Off-Line, At Home: Television, at http://www.yikes.com/~joshm/privacy/offline-home/tv.html (last visited Nov. 27, 2002). Video Privacy Protection Act, 18 U.S.C. § 2710, is an example of legislators reacting to a specific event prompting privacy regulation. See id. Congress passed the Act in response to the controversy that arose when Judge Robert Bork's video rental records were released during his Supreme Court nomination hearings. See id. Outraged by this attack on Judge Bork's privacy, Congress passed the Act, guaranteeing citizens' rental records would not be disclosed to the public. See id. Specifically, the Act prohibits a video rental or sales outlet from disclosing customer rental records without the informed, written consent of the consumer. 18 U.S.C. § 2710 (2000).
B. Federal Legislation: A Sectoral Approach to Regulating Online Privacy

The global growth of the Internet increased congressional awareness of the need to protect online personal information. The federal government, however, maintains only limited authority over the collection and use of personal data collected online. This limitation is a direct result of the federal government’s “sectoral” approach to online privacy and its emphasis on industry self-regulation. Various federal statutes govern the use and disclosure of personally identifiable health information and financial information and protect against the collection of information from children. Despite the existence of laws in these areas, most industries remain unregulated. Without a comprehensive law that addresses all online data collection, consumers face inconsistencies in the amount of privacy protection they actually have. The current federal statutes contribute to this inconsistency by providing individuals with varying degrees of protection.

I. Privacy Legislation in the Health Industry

The growing use of information technology in the management, administration, and delivery of health care led to increasing public concern over the privacy of medical records. The debate over who may access a patient’s medical information, and whether such information can

60. See Kramer, supra note 4, at 400-06.
64. See Gina Marie Stevens, Congressional Research Service, Privacy Protection for Online Information (May 21, 2002) (listing federal privacy laws).
65. See Kramer, supra note 4, at 403 (noting that over the last decade, the Supreme Court has been unable to rule on the issue of data protection, primarily because Congress has not addressed the issue in a comprehensive federal statute).
be used to deny patients employment and insurance, prompted legislative action. To improve the efficiency and effectiveness of the health care system, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which, among other things, provides privacy protection for electronically transmitted health information.

HIPAA provided the Department of Health and Human Services (HHS) with rulemaking authority. Under this authority, HHS issued a final rule in December 2000 that protects the confidentiality of medical records and other personal health information. The rule limits the use and release of individually identifiable health information, gives patients the right to access their medical records, and requires that patients receive written notice describing the types of permissible uses and disclosures of their medical information. Responding to public concern, the privacy rule restricts most disclosures of health information.

68. Id.
70. Id.
71. REDHEAD, supra note 67, at 1-2.
72. Id. at 2. HIPAA gave Congress three years to enact health privacy legislation; otherwise, the Secretary of HHS was required to develop health privacy standards. Id. When Congress failed to meet this deadline, the Secretary issued a comprehensive final regulation to protect the privacy of medical records. Id. Significant modifications to this rule were published on August 14, 2002. Id. at 1. The Health Privacy Rule applies to health care providers who electronically transmit health information in connection with any of the HIPAA-covered transactions, health plans, and health care clearings. See 45 C.F.R. §§ 160.102, 164.500 (2002).
73. See 45 C.F.R. § 164.502(b) (2002).
74. Id. § 164.524.
75. Id. § 164.520.
76. See id. § 164.528. The disclosure procedures that health care providers must follow include providing patients, within sixty days, with an accounting of disclosures over the past six years, except for disclosures for treatment, payment, and health care operations, and for certain other specified purposes. Id. § 164.528(a)(i)-(iv). The accounting must include a brief statement of the purpose of each disclosure and the address of the recipient of the information. Id. § 164.528(b). Disclosures of health information, without a patient’s authorization, may be made for public health purposes as required by state and federal law, to public agencies to conduct health oversight activities, to law enforcement officials pursuant to a warrant or subpoena, in judicial and administrative proceedings, and to researchers provided that a “privacy board” reviews the research protocol and waives patient authorization. Id.
The health privacy rule does not preempt or override state law. Preemption can occur, however, if a state law conflicts with the rule's requirements or provides fewer privacy protections. Most states do not have comprehensive health privacy laws. In addition, most state laws have failed to keep pace with changes in the health care environment or information technology.

2. Privacy Legislation in the Financial Industry

Like the health industry's use of information technology to gather and retain data, financial service businesses began to exploit customer information through electronic means. Privacy concerns developed when businesses began sharing customer data electronically with other providers willing to pay for such data. To address these concerns,

77. See REDHEAD, supra note 67 at 6. Allowing state laws that provide stronger privacy protections to remain in force indicates that the health privacy rule acts as a "federal floor" of minimum privacy protections. Id. Furthermore, the rule defers to state law on the issue of parental notification, thus allowing the disclosure of a minor's health information to a parent if such disclosure is permitted by the state. Id.

78. Id.

79. Health Privacy Project of the Institute for Health Care Research and Policy at Georgetown University, The State of Health Privacy: Key Findings, at http://www.healthprivacy.org/usr_doc/33964.pdf (last visited Nov. 20, 2002) (noting that although most states have some law that addresses the confidentiality of patient health information, few states have anything resembling a comprehensive health privacy law). The notable exceptions include Hawaii, Rhode Island, and Wisconsin, all of which have comprehensive health privacy laws. Id. Furthermore, many state statutes govern health care entities, such as hospitals, but provide no privacy protections regulating health plans or health maintenance organizations (HMOs). Id.

80. Id. The establishment of HMOs as well as statewide health information databases created new demands for data that exceed the limits originally anticipated by the states. Id. Additionally, there are far more entities collecting, receiving, and using health information. Id. For instance, a Department of Motor Vehicles may receive health information from a physician if a patient has a medical condition that requires his or her driver's license to be revoked. Id. Furthermore, certain states – including Arkansas, Colorado, Maine, Minnesota, New York, North Carolina, and Wisconsin – require "hospitals, insurers, and providers to report diagnostic and cost information to public or private state health data clearinghouses. Id.

81. See M. MAUREEN MURPHY, CONGRESSIONAL RESEARCH SERVICE, PRIVACY PROTECTION FOR CUSTOMER FINANCIAL INFORMATION 1 (Oct. 7, 2002). Technology allows financial service businesses to share customer information with others in an effort to offer customers greater access to information about available services. Id.

82. Id. (noting that customers are especially concerned about secondary usage of their personal financial information). Although the Fourth Amendment to the U.S. Constitution requires a search warrant for government access to certain personal financial records such as credit card transactions, it does not protect against governmental access to financial information turned over to third parties. See U.S. CONST. amend. IV.
Congress enacted the Financial Services Modernization Act in 1999, informally known as the Gramm-Leach-Bliley Act (GLBA).\textsuperscript{83}

The primary objective of GLBA is to protect the privacy of consumer information held by financial institutions.\textsuperscript{84} GLBA requires financial institutions to provide privacy notices that explain their information-sharing practices.\textsuperscript{85} In addition, financial institutions must inform customers of their right to "opt-out" if they do not want their information shared with certain nonaffiliated third parties.\textsuperscript{86} Finally, GLBA requires financial institutions to safeguard the security and confidentiality of customer information.\textsuperscript{87}

GLBA's notice and opt-out provisions supplement the obligations imposed by the Fair Credit Reporting Act (FCRA).\textsuperscript{88} Originally enacted in 1970, FCRA ensures that consumer reporting agencies adopt reasonable procedures to meet the legitimate needs for consumer credit information.\textsuperscript{89} FCRA also provides some protection to consumers with respect to the information maintained about them by consumer reporting agencies.\textsuperscript{90} If FCRA requires the financial institution to make clear and

\begin{itemize}
  \item \textsuperscript{83} 15 U.S.C. § 6801 (2000). Title V of the Gramm-Leach-Bliley Act of 1999 reforms the financial services industry, addressing concerns relating to consumer financial privacy. \textit{Id.} Prior to this legislation, individuals did not have much privacy in their financial affairs. \textit{See}, e.g., \textit{United States v. Miller}, 425 U.S. 435, 443 (1976) (holding that there is no constitutionally protected right of privacy in a customer's bank records because these records are the "business records of the bank").
  \item \textsuperscript{84} \textit{See} 15 U.S.C. § 6801 (2000).
  \item \textsuperscript{85} \textit{FTC's Small Business Guide, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act} (stating that consumers have the right to limit some disclosures of their information), \textit{at} http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm (last visited Feb. 9, 2003) [hereinafter \textit{Financial Privacy Requirements of GLBA}].
  \item \textsuperscript{86} 15 U.S.C. § 6802 (2000). GLBA prohibits financial institutions from disclosing nonpublic personal information about consumers to nonaffiliated third parties, unless the institution satisfies various disclosure and opt-out requirements and the consumer has not elected to opt out of the disclosure. \textit{Id.}
  \item \textsuperscript{87} 15 U.S.C. § 6801 (2000).
  \item \textsuperscript{89} 15 U.S.C. § 1681(b) (2000). The reasonable procedures adopted must respect "the confidentiality, accuracy, relevancy, and proper utilization of [consumer credit] information." \textit{Id.}
  \item \textsuperscript{90} \textit{Id.} § 1681(b). The Fair Credit Reporting Act permits distribution of fair and accurate reports. \textit{See id.} § 1681. It requires notification to the subject upon dissemination, imposes time limitations on the disclosure of data, and provides for procedures by which the subject may correct inaccurate information. \textit{See id.} § 1681(b), (d), (f).
\end{itemize}
conspicuous disclosures to consumers regarding the sharing of certain information, then the institution must continue to do so under GLBA.

Enforcement authority under GLBA is delegated to federal banking and security regulators, the Federal Trade Commission (FTC), and state insurance regulators. Each regulatory agency has issued rules implementing the Act's privacy provisions. Finally, GLBA does not expressly preempt state law on financial privacy, but where state law "conflicts with federal law" or is "inconsistent" with federal law, the GLBA controls.

3. Online Privacy Legislation for Children

In a 1998 report to Congress, the FTC documented widespread collection of personal information from young children on the Internet. The FTC stated that collection of personal information from a child under the age of thirteen, without informed parental consent, constitutes a deceptive trade practice. The FTC recommended that Congress pass legislation to protect this vulnerable group.

Congress, agreeing that there was a clear need to provide greater protection for children in the emerging commercial online environment, passed the Children's Online Privacy Protection Act (COPPA) in 1998. COPPA requires parental consent to collect the personal information of children.

91. See Complying with GLBA, supra note 88. FCRA provides that a consumer reporting agency may disseminate a report on a consumer only by obtaining a subpoena or court order, by acquiring consumer consent, or for use in connection with one of several enumerated purposes. 15 U.S.C. § 1681(b) (2000).
92. See Financial Privacy Requirements of GLBA, supra note 85.
93. See Complying with GLBA, supra note 88.
95. See Federal Trade Commission, Online Privacy: A Report to Congress (1998), available at http://www.ftc.gov/reports/privacy3/index.htm (last visited Nov. 20, 2002) [hereinafter Online Privacy Report]. FTC studies found that eighty-nine percent of children's Web sites collected personal information from children. Id. at iii. Forty-six percent of the sites did not disclose their information collection practices. Id. Less than ten percent provided for some parental control over the collection of information from their children. Id.
96. See id. at 4. Personal information collected from children includes name, address, e-mail address, telephone number, and hobbies. Id. at 5; see also Federal Trade Commission, How To Comply With the Children's Online Privacy Protection Rule (Nov. 1999), at http://www.webmastertechniques.com/News2000/COPPA.html (last visited Feb. 2, 2003) (noting that the rule also covers information such as hobbies and interests when they are tied to individually identifiable information).
97. See Online Privacy Report, supra note 95, at iii.
children under thirteen years of age. The law authorizes the FTC to regulate and oversee Web sites targeting children. Operators of Web sites or online services must, among other things, provide notice to parents of their information practices, obtain prior parental consent for the collection, use, or disclosure of personal information from children, and provide a parent, upon request, with the ability to review personal information collected from the child.

4. Other Congressional Attempts To Limit Privacy Invasions on the Internet

a. Amending the Electronic Communications Privacy Act

In 1986, Congress amended the Electronic Communications Privacy Act (ECPA) of 1968 to control online privacy violations. The amended Act prohibits the intentional interception of online communications. Currently, ECPA represents the “most comprehensive data protection legislation that protects personal information on the Internet.”


Parental consent for disclosure of a child’s personal information to either third parties or the public can be obtained in the following ways:

1. Providing a consent form to be signed by the parent and returned to the Web site by postal mail or facsimile;
2. Requiring a parent’s credit card in connection with a transaction;
3. Having a parent call a toll-free telephone number staffed by trained personnel;
4. Using a digital certificate that uses public key technology;
5. Using e-mail accompanied by a [personal identification number] or password obtained through one of the verification methods listed above.

Id. at 12.


101. 15 U.S.C. § 6502(b)(1) (2000). In addition to obtaining initial consent from parents, if a parent withdraws consent at any time, the operator must remove that child’s personal information from the system. See id. § 6502(b)(1)(B)(ii). COPPA also authorizes state attorneys general to file federal actions for violations. See id. 15 U.S.C. § 6504(a)(1). Industry groups or others can create self-regulatory programs to govern participants’ compliance with COPPA. Id. § 6503(a)-(b). These guidelines must include independent monitoring and disciplinary procedures to be submitted to the FTC for approval. Id. An operator’s compliance with Commission-approved self-regulatory guidelines will generally serve as a “safe harbor” in any enforcement action for violations of the rule. Id.

102. Hall, supra note 2, at 637.

103. Id. (noting that the Act is now referred to as the Electronic Communications Privacy Act of 1986). Additionally, the amended Act prohibits “monitor[ing] keystrokes, tap[ping] a data line, or rerout[ing] an ‘electronic communication to provide contemporaneous acquisition.’” Id. at 637-38.

104. Tan, supra note 42, at 671.
Communications providers must abide by ECPA’s provisions outlawing electronic surveillance and the use of information secured through electronic surveillance. Most importantly, ECPA prohibits unauthorized access to stored electronic communications as well as unauthorized interception of messages in transmission.

b. Privacy Legislation for the Public Sector

The Privacy Act of 1974 represents an attempt by Congress to provide personal privacy protection in federal agency operations and practices. It applies to a wide variety of records maintained by federal agencies and protects privacy interests by regulating the government’s collection, use, and dissemination of personal information. The Privacy Act attempts to structure how information is processed within the public sector through the regulation of recordkeeping and disclosure practices.

106. Id. The United States District Court for the District of Columbia relied upon the ECPA to find that the Navy’s actions in requesting the name of an AOL subscriber without a warrant were illegal. McVeigh v. Cohen, 983 F. Supp. 215, 219-20 (D.D.C. 1998). In McVeigh v. Cohen, the court held that the ECPA forbids the federal government from seeking information about online communications system users unless “it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or . . . it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question.” Id. at 219.

108. See id. § 552a(b). The Act provides that “an agency may not disclose any record regarding an individual to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” Id.
109. See id. §§ 552a(e)(1), (5). The Act provides that agencies must maintain in their records only information that is “relevant and necessary” to accomplish a purpose of the agency, as well as maintain all records used by the agency in making any determination about an individual in such a way as to assure fairness to the individual in that determination. Id. The Act further requires agencies to establish safeguards to ensure the security and confidentiality of records. Id.; see also Schwartz, supra note 16, at 583 (noting
Furthermore, under the Act, individuals have certain rights and remedies, including the right to access agency records containing their personal information and the right to request correction of information that is inaccurate, irrelevant, or incomplete.110

C. Self-Regulation: FTC Recommendations for Industries Regarding Online Privacy Protection

1. The Emergence of Fair Information Practices

In addition to passing various privacy laws to address consumer concerns, the federal government also promotes industry self-regulation.111 Since 1995, the FTC has had a major presence in the public debate concerning online privacy.112 As the federal government’s primary consumer protection agency, the FTC has encouraged and evaluated self-regulatory efforts to enhance consumer privacy.113 In one particular survey, the FTC examined the privacy practices of numerous Web sites and assessed industry efforts to implement self-regulatory programs.114 The surveys indicated that the majority of online businesses failed to adopt basic privacy principles.115 Thus, the FTC concluded that the self-regulatory system was ineffective.116

In subsequent FTC reports, the basic privacy principles were honed into four widely accepted fair information practices: notice, choice, access, and security.117 The most “fundamental principle” ensures that

---

110. See 5 U.S.C. § 552a(d)(1), (2).
111. See Tan, supra note 42, at 674-75 (noting online industry’s efforts to self-regulate fall short of protections needed to protect Internet users).
113. See id.
114. See id.
115. See id.
117. According to the FTC, these principles are “essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests.” Federal Trade Commission, Fair
consumers receive "notice of an entity's information practices before any personal information is collected."\textsuperscript{118} The second principle is consumer choice or consent, which provides consumers with "options as to how any personal information collected from them may be used."\textsuperscript{119} Access, the third core principle, refers to an individual's ability both to access personal data and to contest that data's accuracy.\textsuperscript{120} The fourth principle mandates the security of any information that an online entity collects.\textsuperscript{121} In its most recent report on online privacy, the FTC recommended that Congress enact legislation requiring consumer-oriented commercial Web sites that collect personally identifying information to comply with the fair information principles.\textsuperscript{122}

2. Privacy Policies

In addition to encouraging compliance with the fair information principles, the FTC urges commercial Web sites to post privacy policies

\textsuperscript{118}See STEVENS, supra note 37, at 5.
\textsuperscript{119}Id. Two options exist for consumers to provide consent. See Kramer, supra note 4, at 408-09. One option, referred to as the "opt-in" approach, requires consumers to provide consent before companies can collect or disclose personal information. See id. Under the alternative "opt-out" option, companies are free to collect or disclose personal information unless the consumer indicates otherwise. See id. Industry prefers the opt-out option because the burden of removing personal information falls on the consumer. See id. However, consumers find the opt-out approach time-consuming and difficult if the company makes the option hard to locate. See id. at 409. The opt-in versus opt-out debate is a significant hurdle that privacy advocates and industry must overcome in order to pass comprehensive privacy legislation. See id. at 408-09.
\textsuperscript{120}See STEVENS, supra note 37, at 15.
\textsuperscript{121}See id.
\textsuperscript{122}See Privacy Online Hearing, supra note 112. Legislation based upon these core principles attempts to provide a solution to privacy problems posed by collection of personal information online. See STEVENS, supra note 37, at 15. Following this recommendation, the Commission conducted a survey, which found that in a random sample of 335 Web sites that collect personally identifying information, only twenty percent implement the fair information practice principles. See Privacy Online Hearing, supra note 112. The disappointing results of this survey prompted the Commission to recommend that Congress enact legislation to establish basic standards of practice for the collection of information online. See id.
that identify their information collection practices. The intent of these privacy policies is to inform users about what happens to the personal information they provide. In order for such a privacy policy to be effective, two additional elements are necessary. First, "the policy must be protective." Second, the "privacy policy must be followed" by the Web site. In essence, posting a privacy policy alone does not ensure adequate privacy protection for consumers.

Although it is not a privacy statute, Section 5 of the Federal Trade Commission Act can be used by the FTC to address deceptive online information practices. A typical FTC enforcement action addresses a company's failure to comply with its stated privacy policy. While FTC enforcement measures provide some protection to consumers, this case-

125. Id.
126. Id. (noting that "a privacy policy in which a company states that it shares any and all user information with any third party that asks for it is essentially a useless privacy policy").
127. Id.
128. Surfer Beware, supra note 6.
130. See Complaint, In re Geocities, Docket No. C-3850 (Feb. 1999) (alleging that a popular site sold personal information to third party marketers, violating a provision in its privacy policy), available at http://www.ftc.gov/os/1999/9902/9823015cmp.htm (last visited Oct. 1, 2002); see also Complaint, FTC v. Toysmart.com, LLC, and Toysmart.com, Inc. (Civil Action 00-11341-RGS) (D. Mass. 2000) (challenging a Web site's attempts to sell personal customer information gathered pursuant to a privacy policy that promised that such information would never be disclosed to a third party), available at http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm (last visited Oct. 1, 2002); Complaint, FTC v. Sandra Rennert, et al., No. CV-S-00-0861-JBR (D. Nev. 2000) (alleging that defendants misrepresented the security and encryption used to protect consumers' information and claimed that the defendants used the information in a manner contrary to their stated purpose), available at http://www.ftc.gov/os/2000/07/iogcomp.htm (last visited Apr. 11, 2003); Complaint, In re Microsoft, File No. 012 3240 (alleging that through Microsoft's Passport, an online ID service that lets users enter one name and password when using the Internet, the company failed to take necessary precautions to protect consumers' personal information from leaking out), available at http://www.ftc.gov/os/2002/08/microsoftcmp.pdf (last visited Oct. 1, 2002); Complaint, In re Liberty Financial, File No. 982 3522, (alleging that the Web site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously), available at http://www.ftc.gov/os/1999/9905/ibrtycmp.htm (last visited Oct. 1, 2002).
by-case approach allows many Web sites to continue deceptive practices without any legal repercussions. Following the advice of the FTC, Congress is currently considering legislation that would support the fair information principles and require effective privacy policies.

D. Comprehensive Privacy Legislation Currently Under Debate

Comprehensive online privacy legislation would increase consumer confidence in the Internet by establishing a clear set of rules about how personal information is collected and used. Additionally, federal legislation would provide consistent regulation of information collection practices across all fifty states. During the 107th Congress, two bills were introduced to provide consumers with greater security when using the Internet.

1. The Online Personal Privacy Act

On April 18, 2002, Senator Ernest Hollings (D-S.C.) introduced S. 2201, the Online Personal Privacy Act (OPPA). The primary purpose

---

131. See Muris, supra note 11 (announcing FTC plans to enforce privacy promises). The FTC will expand its review of privacy policies and ensure that restrictions on disclosures to third parties are honored. See id.

132. Online Privacy Report, supra note 95. For the most part, Internet sites have responded to the FTC's efforts to encourage posting privacy policies. See id. at ii-iii. In 2000, virtually all of the top 100 sites had notices. Id. However, complying with these policies proves problematic for companies that are sold or reorganized. Muris, supra note 11.

133. See Privacy Online Hearing, supra note 112 (indicating that technological advancements in information collection and use have increased consumer concerns regarding online privacy). A 2000 survey showed that ninety-two percent of consumers are “concerned about the misuse of their personal information online.” Id. Another study revealed that ninety-two percent of respondents from online households do not trust online businesses to keep personal information secure. See Steve Lohr, Survey Shows Few Trust Promises on Online Privacy, N.Y. TIMES, Apr. 17, 2000, at C4; see also Nola Young, Privacy Laws Could Help E-Commerce To Grow, KITCHENER-WATERLOO REC., June 12, 2002, at F2, available at 2002 WL 22074263 (noting that although online consumer shopping is increasingly popular, there are still many consumers who opt not to use the Internet when making purchases because they fear that the information they provide will be misused).

134. See generally SMITH ET AL., supra note 13 (providing an overview of pending legislation that would establish a national set of privacy policies).


The Struggle To Keep Personal Data Personal

of this proposed bill is to strengthen privacy protection for online consumers by establishing a uniform federal standard for the protection of online personal information. To achieve this goal, the bill prohibits any online entity from collecting or disclosing a user's "personally identifiable information" – including the user's name, address, phone number, and e-mail address – without a "clear and conspicuous" user notice. Most importantly, the bill codifies the core privacy protection principles outlined by the FTC.

The bill creates two categories of personally identifiable information: sensitive information and nonsensitive information. "Sensitive personally identifiable information" includes an individual's financial information, medical information, ethnic information, religious affiliation, sexual orientation, political party affiliation, and Social Security number. In contrast, "nonsensitive personally identifiable information" includes all other information not defined as sensitive information, such as name, address, and online purchases of clothing. Internet companies must obtain affirmative consumer consent before collecting, using, or disclosing sensitive information; however, companies need only provide consumers with an opportunity to opt out of nonsensitive information sharing. In addition, an Internet company

also Sharon Gaudin, Controversial Online Privacy Bill Advances in Senate, IT MANAGEMENT, May 22, 2002, at http://itmanagement.earthweb.com/secu/print/0,,11953_1143011,00.html (last visited Oct. 7, 2002) (noting that with approval from the Senate Commerce Committee, the bill passed a critical test). On August 1, 2002, S. 2201 was reported to the Senate, the latest major action taken on this bill. See Thomas Legislative Information on the Internet, at http://thomas.loc.gov (last visited Nov. 20, 2002). Currently, the bill has ten co-sponsors. Id.

137. CBA Reports, Senate Committees Moving on Privacy Bills, June 1, 2002, available at 2002 WL 9025486.


139. S. 2201, §§ 102, 105, 106.

140. S. 2201, § 102(b), (c).

141. S. 2201, § 401(15); see also Gaudin, supra note 136 (noting that sensitive personal information includes an individual's debts, income, assets, and medical records).

142. Committee Approves Online Personal Privacy Act, S. 2201, supra note 136.

143. S. 2201, § 102(b), (c). In other words, consumers must opt in to sharing sensitive information. Id. § 102(b). Nonsensitive information requires "robust notice" in addition to clear and conspicuous notice. Id. § 102(c). "Robust notice" is defined as "actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the Internet service provider, online service provider, or operator of a commercial [W]ebsite to use or disclose that information for marketing or other purposes." Id. § 401(13). Many Internet companies are doing this already; for example, the Web site for "1-800 Flowers" states in its privacy policy: "If you prefer not to have us provide personal information about you to third parties . . . please let us know by either writing us . . . or e-mailing us." Furthermore, the Web site states: "Your instructions will apply to information collected by 1-800-FLOWERS.COM, not to information collected on other Web sites or companies owned by [us]. If you are a user of any of those Web sites
must provide users with notice if the company changes its privacy policy or engages in a breach of that policy. In accordance with the fair information practices, the bill requires online operators to provide individuals with “reasonable access” to their personal information. To address security, Internet companies must “establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personally identifiable information.” Finally, the bill establishes a uniform federal standard for online privacy protection by preempting state Internet laws. During the 2002 congressional session, and wish to opt-out in a similar manner . . . please go to those sites.” 1-800 Flowers.com, at http://www.1800flowers.com/security/index.asp (last visited Apr. 22, 2003). Similarly, NBC’s Web site states: “NBC . . . share[s] personal information with . . . third parties. NBC will try to provide users with an opportunity to decline this service when such information is requested from [the user] online.” NBC.com, at http://www.nbc.com/nbc/footer/Privacy_Policy.shtm. (last visited Apr. 22, 2003).

144. See S. 2201, § 103, 107th Cong. (2002).

145. Id. § 105(a)(1). This right of reasonable access is not unqualified. See id. § 105(a)(1), (c). Rather, it considers a variety of factors, including the sensitivity of the information sought by the consumer as well as the burden and expense on the provider in giving consumers access to their personal information. See id. § 105(c). In addition, the bill would permit online companies to charge individuals a reasonable fee to access their personal data. Id. § 105(d). It further provides that individuals must be given a “reasonable opportunity” to correct or delete information maintained by the Internet company. Id. § 105(a)(2). But see Gaudin, supra note 136. Some online businesses express concern that the bill’s access provision would contribute to “expensive overhauls of e-commerce systems and databases, and create security nightmares by letting customers into the system to check – and change – their personal information.” Id.

146. S. 2201, § 106. The bill grants the FTC enforcement and rulemaking power. See id. § 201. Additionally, the bill provides legal remedies for states if online operators improperly release a resident’s information. See id. § 206 (noting that state attorneys general may bring civil actions on behalf of their residents). Finally, individuals may bring a private right of action if any online service provider fails to abide by the terms of the law with respect to sensitive personally identifiable information. See id. § 205 (limiting the action to $500 in damages). The bill provides a safe harbor. See id. § 203. If an online provider is a participant in a self-regulatory program approved by the FTC and is in full compliance with such programs, then the provider is also in compliance with the requirements of this bill. See id. (stating that the FTC, every two years, is required to reevaluate its approval of each program). Furthermore, it is possible to appeal an FTC decision not to approve a program. Id.

another bill similar in purpose, but different in application, was also introduced.148

2. The Consumer Privacy Protection Act

Twenty days after Senator Hollings introduced the Online Personal Privacy Act, Representative Cliff Steams (R-Fla.) introduced H.R. 4678, the Consumer Privacy Protection Act (CPPA) of 2002.149 CPPA applies to “data collection organization[s]” gathering data by any means.150 The bill requires each business to give customers notice of the use of personally identifiable information, both at the time of data collection and upon a change in the organization’s privacy policy.151 Personally identifiable information includes first and last name, home address, e-mail address, telephone number, Social Security number, and “any other unique identifying information.”152 Furthermore, users may exercise their right to “opt out” of the use or sharing of personal information.153

The bill includes a provision requiring companies to develop information security programs, but it does not specifically require that security and confidentiality be maintained.154 It grants the FTC the sole power to enforce the regulations.155 Additionally, the bill does not

149. See id. The Consumer Privacy Protection Act was introduced in the House of Representatives on May 8, 2002. Id. On the same day, the bill was referred to the House Committee on Energy and Commerce as well as the Committee on International Relations. Thomas Legislative Information on the Internet, at http://thomas.loc.gov (last visited Nov. 20, 2002). On May 17, 2002, the bill was referred to the Subcommittee on Commerce, Trade, and Consumer Protection. Id. The latest action on this bill occurred on September 24, 2002 when subcommittee hearings were held. Id. Currently, H.R. 4678 has twenty-one co-sponsors. Id.
150. See H.R. 4678, §§ 101(a), 401(3)(A). A “data collection organization” is defined as “an entity (or an agent or affiliate of the entity) that collects (by any means, through any medium), sells, discloses for consideration, or uses personally identifiable information of the consumer.” Id. § 401(3)(A).
151. Id. § 101(a).
152. Id. § 401(4)(A)–(B). Personally identifiable information does not include “anonymous or aggregate data, or any other information that does not identify a unique living individual; information about a consumer inferred from data maintained about a consumer; or information about a consumer obtained from a public record.” Id. § 401(4)(C).
154. See H.R. 4678, § 105(a), (b).
155. See H.R. 4678, § 107. A violation of the provisions under Title I is considered an “unfair or deceptive act or practice unlawful under Section 5(a)(1) of the Federal Trade Commission Act.” Id. The FTC’s enforcement power allows it to “issue generally
modify, limit, or supersede specified federal privacy laws, including COPPA, GLBA, and HIPAA. Compliance with relevant sections of existing federal privacy laws satisfies the provisions in the bill. Finally, the CPPA provides for a study of the impact of information privacy laws, regulations, or agreements enacted by other nations on the interstate and foreign commerce of the United States.

II. THE INADEQUACIES OF EXISTING PRIVACY LAWS AND HOW S. 2201 AND H.R. 4678 PROVIDE BETTER PROTECTION

A. Is Federal Reform the Answer?

Despite the existence of federal law limiting personal information collection practices, decreasing consumer confidence in the privacy of personal data continues to affect the online industry negatively. Without comprehensive federal standards mandating compliance by all persons and entities collecting personal information, dissatisfaction and mistrust of online business practices will likely continue to grow.

applicable guidelines and, upon request, advisory opinions . . . but may not prescribe regulations to carry out this title.” Id. Additionally, the FTC may take necessary action if consumers have a reasonable belief that they are victims of identity theft. Id. § 201. There is no provision granting a private right of action, nor is there a provision allowing enforcement action by states. See id.


157. Id. § 109(a).

158. Id. § 301. If findings conclude that such information privacy laws, regulations, or agreements substantially impede interstate and foreign commerce of the United States, the Secretary of Commerce is permitted to take all steps necessary to mitigate against such discriminatory impact. Id. § 302.

159. See Letter from Mozelle W. Thompson, Federal Trade Commission, to John McCain, U.S. Senator (April 24, 2002), available at http://www.ftc.gov/os/2002/04/sb2201thompson.htm (last visited Mar. 28, 2003). Ms. Thompson states that “[c]onsumer confidence is one of the most important features of American economic strength and, as demonstrated by recent declines in dot-com industries, emerging markets and young industries are particularly vulnerable to consumer uncertainty.” Id.

160. See id. (noting that a survey conducted by Forrester Research in 2001 found that seventy-three percent of online consumers who refused to purchase online did so because of privacy concerns). Without federal standards, it will be difficult to provide consumers with adequate protection from crimes such as identity theft. See W.A. Lee, Marketing Spin on Customers’ Privacy Jitters, 167 AMERICAN BANKER 166, Aug. 29, 2002. A recent study by Celent Communications predicted that in the year 2006, twenty-five percent of identity theft cases will be the result of online transactions. Id. As one of the fastest
Without federal reform, sectoral legislation will proliferate, leaving bigger gaps in privacy protection for online transactions.\(^\text{161}\) As FTC studies have shown, the online industry has been unable to self-regulate effectively.\(^\text{162}\) Privacy notices are an ineffective means of protection because Internet companies continually violate their own policies.\(^\text{163}\) The absence of comprehensive legislation allows many online businesses to violate consumer trust because they remain unreachable by agencies like the FTC.\(^\text{164}\) Without legislation, “too much of the risk associated with e-commerce is shifted to the consumer at a time when consumer confidence is critical.”\(^\text{165}\) Federal legislation offers uniformity and predictability that would substantially increase consumer confidence in online transactions.\(^\text{166}\)

**B. Gaps Left by Existing Laws**

The sectoral approach used by Congress has left several gaps in online privacy protection.\(^\text{167}\) Inconsistencies exist in the types of information protected and the categories of people who may access it.\(^\text{168}\) As a result, various privacy laws prove burdensome for businesses and confusing for consumers.\(^\text{169}\)

---

\(^{161}\) See generally A Review of State and Federal Privacy Laws, supra note 147.

\(^{162}\) See Online Privacy Report, supra note 95; see also Self-Regulation, supra note 116.

\(^{163}\) See supra note 130 and accompanying text.


\(^{165}\) Letter From Mozelle W. Thompson, supra note 159; see also Privacy Online Hearing, supra note 112.


\(^{167}\) See A Review of State and Federal Privacy Laws, supra note 147.

\(^{168}\) See id.

\(^{169}\) See Letter from Mozelle W. Thompson, supra note 159.
Several problems persist in existing privacy statutes, such as COPPA, GLBA, and HIPAA. For example, many Web site sponsors required to comply with COPPA are unaware that the statute applies to them. Although COPPA is directed at child-oriented Web sites, it also covers all general-audience Web sites that knowingly collect information from children under the age of thirteen. COPPA applies to Web sites "that receive e-mail from users who identify themselves as children and sites where children post their age in e-mail messages, instant messages, bulletin boards or Web pages." Unfortunately, this practice encourages children to lie about their ages. Furthermore, children are visiting more "risky sites because 'safe sites' like Disney have added many restrictions" in order to comply with COPPA.

In addition, it is alleged that GLBA has not increased financial privacy. For example, "the amount of financial data that financial institutions can collect has increased rapidly" since the bill's enactment. In addition, most of the information sharing "is done without the knowledge or approval of the customers." This practice is largely attributable to unclear and unreadable opt-out notices provided by financial institutions. Moreover, not all individuals are entitled to receive privacy notices. Financial institutions are only required to provide "customers" with a privacy notice, while "consumers" are not entitled to such notice. Generally, if the relationship between the


171. Id. Lawyer Parry Aftab, author of The Parents' Guide to Protecting Your Children in Cyberspace, echoes the belief that many Web sites do not realize they must comply with COPPA's provisions. James Niccolai, Teething Problems Hit Online Child Protection Plan, IDG NEWS SERVICE (Apr. 21, 2000), at http://www.idg.net (last visited Nov. 18, 2002). According to Aftab, "[a] lot of people think the law applies to children's sites only, but it doesn't." Id.

172. Marsan, supra note 170.

173. See Niccolai, supra note 171.


175. See Hubbard, supra note 57.

176. Id. (quoting Senator Paul Sarbanes, Former Chairman of the Senate Banking Committee).

177. Id.

178. Id.


180. See id. § 6801(a). Consumers are only entitled to receive privacy notices if the financial institution shares the consumers' information with companies not affiliated with it, with some exceptions. See id. § 6802(a), (e).
The Struggle To Keep Personal Data Personal

financial institution and the individual is significant or long-term, a customer relationship exists.\textsuperscript{181} GLBA also protects an individual’s “nonpublic personal information,” which is defined as “personally identifiable financial information.”\textsuperscript{182} GLBA does not specify, however, what “personally identifiable financial information” includes.\textsuperscript{183}

In the health industry, inconsistent compliance with the privacy provisions of HIPAA is proving troublesome.\textsuperscript{184} Because some states abide by the privacy rule while others do not, problems exist when, for example, a telemedicine specialist at a hospital in one state confers with several patients in different states.\textsuperscript{185} Determining which state law is the most stringent for privacy is a difficult and burdensome task.\textsuperscript{186} Thus, COPPA, GLBA, and HIPAA fall short of effectively implementing the fair information principles established by the FTC.

Problems have arisen with other statutes as well. ECPA, for example, contains several exceptions, making the law complex and leaving gaps in the amount of privacy protection provided.\textsuperscript{187} First, online services can effectively review private e-mail messages due to the storage systems the services utilize.\textsuperscript{188} Second, online services may legally view and disclose private messages if either the sender or recipient consents.\textsuperscript{189} Third, online services may be required to disclose private information in response to a court order or subpoena.\textsuperscript{190} Fourth, employers may inspect the contents of employee e-mails, suggesting that any e-mail sent from a

\textsuperscript{181} See id. § 6809(11). The term “consumer” is defined as “an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes.” Id. § 6809(9).

\textsuperscript{182} Id. §§ 6801, 6809(4)(A).

\textsuperscript{183} See id. § 6809(4)(A).


\textsuperscript{185} Id.

\textsuperscript{186} Id. (noting that all fifty states have laws governing the use and disclosure of health information). As a result, there are varying degrees of protection among the laws. Id.

\textsuperscript{187} Rules of the Road, supra note 123 (noting that the ECPA makes a distinction between messages in transit and those stored on computers). As a result, stored messages are afforded less protection than messages intercepted during transmission. Id.

\textsuperscript{188} Id.

\textsuperscript{189} Id.

\textsuperscript{190} Id.; see also 18 U.S.C. § 2703 (2000) (noting that messages less than 180 days old can be accessed by a government agent who obtains a proper warrant). If the message has been stored for over 180 days, the government agent need only obtain an administrative subpoena. 18 U.S.C. § 2703(a)-(b) (2000). It is also notable that system operators who obey government agents with proper court documentation are not held subject to legal action by users whose messages are seized by the government. Id. § 2703(e).
business location is most likely not private. Finally, the USA PATRIOT Act, recently passed by Congress in response to the terrorist attacks of September 11th, reduces the checks and balances of ECPA regarding law enforcement access to online activity records.

Like ECPA, the Privacy Act has been amended on several occasions, but it has been suggested that the new provisions are no longer effective

191. See Rules of the Road, supra note 123. A significant gap left by sectoral legislation is the lack of safeguards against workplace monitoring. A Review of State and Federal Privacy Laws, supra note 147 (noting that there is no law regarding workplace monitoring at either the federal or state level). The focus of the debate on workplace monitoring is whether companies must provide notice to their employees of what monitoring takes place. MARCIA S. SMITH, CONGRESSIONAL RESEARCH SERVICE, INTERNET PRIVACY: AN ANALYSIS OF TECHNOLOGY AND POLICY ISSUES 26 (Dec. 21, 2000). According to a 2001 survey by the American Management Association, “nearly eighty percent of employers engage in electronic monitoring of employees' work-related communications and activities.” Douglas M. Towns, Legal Issues Involved in Monitoring Employees' Internet and E-Mail Usage, at http://www.gigalaw.com/articles/2002-all/towns-2002-01-all.html (last visited Sept. 23, 2002). This includes monitoring employees' e-mail or Internet usage. See id. The federal legislation “most relevant” to employee privacy protection is ECPA. S. Elizabeth Wilborn, Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace, 32 GA. L. REV. 825, 839-841 (1998). While ECPA prohibits the intentional interception of electronic communications, technological advances, such as electronic mail monitoring, weaken the statute’s effectiveness. See id. at 841. But see McVeigh v. Cohen, 983 F. Supp. 215, 221-22 (D.D.C. 1998) (relying upon the ECPA, the U.S. District Court for the District of Columbia held that the Navy’s actions in requesting the name of an AOL subscriber without a warrant were illegal). In addition, ECPA contains loopholes that facilitate employee monitoring. See Wilborn, supra, at 840-41. ECPA does not require prior notice to employees and permits employers to intercept communications where there is actual or implied employee consent. See 18 U.S.C. § 2511(2)(d) (2000) (allowing interception of electronic communications where one party to communications has given prior consent, either express or implied, to such interception); see also, Electronic Privacy Information Center, Workplace Privacy, (noting that “consent has been found where [the] employer merely gives notice of the monitoring”), at http://www.epic.org/privacy/workplace/default.html (last visited Sept. 23, 2002). Furthermore, employers are permitted to monitor networks for business purposes. 18 U.S.C. § 2510(5)(a) (exempting from definition of interceptions those occurring “in the ordinary course of . . . business”). This enables employers to view employees’ e-mail as long as this surveillance is within the “ordinary course of business.” See id. It is often difficult to prove that any monitoring scheme that enhances productivity or efficiency is not within this limitation. See Burnett v. State, 789 S.W.2d 376, 378-79 (Tex. App. 1990) (holding that monitoring of personal telephone calls was justified because “it is in the ordinary course of business for an employer to take measures to avoid the theft of its merchandise); see also Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (finding that the defendant employer had acted in the ordinary course of business when it monitored employee phone calls because the employer had reason to suspect that its employee was discussing confidential information with a former employee).

192. See Rules of the Road, supra note 123 (indicating that the USA PATRIOT Act also expands the types of records that can be sought without a court order).
for data protection. The continuance of unlawful disclosures of personal information to third parties indicates that better oversight and enforcement of the Privacy Act are necessary. To achieve effective oversight and enforceability, some advocate the establishment of a Chief Information Officer of the United States (CIOUS) or a small privacy agency. Another issue concerns the “routine use” clause of the Privacy Act, which requires agencies to alert citizens as to how personally identifiable information will be used. Although such notices are published in the Federal Register, most citizens are unaware of their existence and implications. Modifying the “routine use” clause would improve citizen awareness of how the government might use their personal information. A final issue concerns whether the Act should have broader application. Congress and legislative support agencies are currently not subject to the Act’s provisions, which raises questions as to what extent, if any, the legislative branch should be subject to the Act.

C. How OPPA and CPPA Fill Gaps Left by Sectoral Legislation

It is evident that several gaps remain in privacy protection as a result of Congress’ sectoral approach to regulating the disposition of personally

193. HAROLD C. RELYEA, CONGRESSIONAL RESEARCH SERVICE, THE PRIVACY ACT: EMERGING ISSUES AND RELATED LEGISLATION 1 (updated Feb. 26, 2002). The most noteworthy amendment is the Computer Matching and Privacy Protection Act of 1988. See Schwartz, supra note 16, at 581-88. This Act regulates the federal government’s data matching, the “electronic comparison of two or more sets of records in order to find individuals included in more than one database.” Id. at 587.

194. RELYEA, supra note 193, at 5. A 2000 General Accounting Office report indicated that twenty-three out of seventy agencies “had disclosed personal information gathered from their [W]eb sites to third parties.” Id. The report revealed that four agencies were found to be sharing such information with private organizations. Id.

195. Id. at 7. Proponents of this new position contend that “many aspects of information technology (IT) management would benefit from having an IT [sic] expert in charge . . . [and] that such an official would better facilitate [Office of Management and Budget] oversight of IT applications and use.” Id.

196. Id. at 9.

197. Id.

198. Id. Until now, the routine use clause has been interpreted broadly, allowing agency officials great ability to move data among federal agencies. Id.

199. See Review of State and Federal Privacy Laws, supra note 147. The Act only covers the public sector and does not touch on the private sector. Id. While many people have the misconception that the Act covers every situation in which personally identifiable information is collected, in reality it only covers “citizens’ relationships with federal government agencies.” Id.

200. RELYEA, supra note 193, at 7-8 (noting that the White House Office and the Office of the Vice President are currently not within the scope of the Privacy Act).
identifiable information.\textsuperscript{201} A comprehensive federal law, such as OPPA or CPPA, would fill the gaps and provide a clear set of privacy standards.\textsuperscript{202} A law that addresses all online transactions will prevent multiple standards that inevitably Balkanize e-commerce.\textsuperscript{203}

The broader coverage of both OPPA and CPPA would clarify for many Web sites whether they must comply with privacy provisions.\textsuperscript{204} In addition, the proposed bills do not distinguish between individuals entitled to receive privacy notices.\textsuperscript{205} Instead, notice is required in all instances when "personally identifiable information" is collected.\textsuperscript{206} To assist practitioners facing a patchwork of state privacy standards, OPPA and CPPA preempt state privacy laws.\textsuperscript{207} Furthermore, both establish strong safeguards that should diminish public concern about privacy.\textsuperscript{208}

Most importantly, the provisions of OPPA and CPPA focus on the fair information principles.\textsuperscript{209} Both bills set forth the principle that use of personal data should be consistent with privacy policies unless the consumer consents to alternative uses.\textsuperscript{210} The bills require that any change in privacy policies be communicated to the user, taking the burden off consumers to track such changes themselves.\textsuperscript{211} Thus, both OPPA and CPPA address many of the delicate problems associated with a legislative privacy framework.\textsuperscript{212}

\textbf{D. Mirror, Mirror, On the Wall, Which Bill Provides the Greatest Protection of Them All?}

Both OPPA and CPPA propose to regulate the use of personal information on the Internet.\textsuperscript{213} OPPA, however, is a more balanced,
comprehensive approach to protecting consumer privacy online.\textsuperscript{214} CPPA does not include all the fair information principles needed to render it an effective privacy law.\textsuperscript{215} To its detriment, CPPA does not grant individuals access to the personal information collected or the opportunity to amend such information when incorrect.\textsuperscript{216} OPPA, in contrast, gives individuals access to their personal information, allows individuals to correct inaccurate information, and maintains data only to the extent necessary for the purposes for which the data is to be used.\textsuperscript{217} The reasonableness test incorporated in this law strikes an appropriate balance among the competing interests of consumer privacy, the relative sensitivity of different types of personal information, and the burdens and costs imposed on the Web site operator.\textsuperscript{218}

OPPA favors consumer interests by requiring companies to obtain affirmative customer consent before sharing sensitive data.\textsuperscript{219} This approach, as opposed to CPPA's opt-out option, guarantees consumer notice and compels the information collector to clarify its practices before the consumer agrees to them.\textsuperscript{220} It also effectively equalizes the bargaining position of consumers and online merchants in the market for personal information.\textsuperscript{221} Privacy legislation for the financial services industry has shown that the opt-out system produces privacy notices that do not command attention, are hard to understand, and have different, and sometimes difficult, procedures for opting out.\textsuperscript{222} Another advantage


\textsuperscript{215} See generally H.R. 4678, §§101-110 (providing measures regarding notice, consent, security, and enforcement, but no provision exists for consumer access to personal information).

\textsuperscript{216} Compare H.R. 4678, §§ 101-110, with S. 2201, § 105.

\textsuperscript{217} S. 2201, § 105; see also Online Personal Privacy Act of 2002, Hearing on S. 2201, Before the Senate Comm. on Commerce, Science, and Transportation, 107th Cong. (2002) (statement of Marc Rothenburg, Executive Director, Electronic Privacy Information Center) (explaining the fair information practices that are included in OPPA) [hereinafter OPPA Hearing], at http://www.epic.org (last visited Oct. 1, 2002). The bill's access provision requires that copies of consumer information must be available at a "reasonable fee." \textit{Id.} at 3. The fee can be waived in situations where an individual is unable to pay or where fraud has been a factor. \textit{Id.}

\textsuperscript{218} See S. 2201, § 105(c).

\textsuperscript{219} See S. 2201, § 102(b). The permanence of the consent provision found in OPPA provides that a consumer's privacy preferences stay with the user despite corporate changes. See \textit{id.} §102(c).

\textsuperscript{220} Compare S. 2201, § 102(b), with H.R. 4678, § 101-103.

\textsuperscript{221} See SMITH, \textit{supra} note 191, at 12 (stating that the opt-out approach often puts the consumer at a disadvantage because Web sites make it difficult to locate where on the site a user should indicate that he does not want his information shared with others).

\textsuperscript{222} See Hubbard, \textit{supra} note 57.
of OPPA is that it creates categories for handling information, a distinction that businesses typically make and a practice that is currently evolving. OPPA recognizes that some highly sensitive personal information, such as medical information or a person's religious beliefs, are clearly more sensitive than other garden-variety types of information, such as a person's name or e-mail address. See S. 2201, §§ 401(11), (15). This two-category approach is also "found in Europe and other regions of the world to make clear that a stronger privacy standard should apply to more sensitive personal information." OPPA Hearing, supra note 217.

226. Compare S. 2201, §§ 102, 401 with H.R. 4678, § 401. OPPA recognizes that some highly sensitive personal information, such as medical information or a person's religious beliefs, are clearly more sensitive than other garden-variety types of information, such as a person's name or e-mail address. See S. 2201, §§ 401(11), (15). This two-category approach is also "found in Europe and other regions of the world to make clear that a stronger privacy standard should apply to more sensitive personal information." OPPA Hearing, supra note 217.


228. Compare S. 2201, with H.R. 4678.

229. S. 2201, § 204; see also SMITH ET AL., supra note 13, at 11.


the Internet.\textsuperscript{232} By incorporating the fair information principles, it creates a level playing field for both consumers and industry.\textsuperscript{233}

III. PRACTICAL BENEFITS OPPA WILL BRING IF PASSED

As the nation wages war on global terrorism, it is imperative for Congress to continue considering the matter of information privacy.\textsuperscript{234} OPPA is reflective of a “real world” consumer environment.\textsuperscript{235} The balanced approach to privacy that OPPA provides will promote consumer confidence in online transactions, encourage online shopping, and “give much needed support to the lagging high-tech industry.”\textsuperscript{236} This is critical to the growth of e-commerce and the online marketplace.\textsuperscript{237} The bill also considers the inevitability of technological growth by allowing for flexibility and change.\textsuperscript{238} Not only will OPPA assist consumers, but online businesses will benefit as well.\textsuperscript{239} The bill’s consistent legal framework ensures that businesses will no longer be burdened by conflicting privacy standards.\textsuperscript{240} OPPA recognizes the need to balance the vital privacy interests of consumers with the economic and financial interests of e-business.\textsuperscript{241} Thus, OPPA offers a beneficial solution for both consumers and businesses.\textsuperscript{242}

OPPA provides strong protection measures for consumers in the online world.\textsuperscript{243} Consumer participation in the online world should not be conditioned on a willingness to relinquish control over personal information.\textsuperscript{244} OPPA establishes baseline consumer protections that will eliminate the difficult situation where consumers are forced to choose between disclosing personal information or not using the Internet at all.\textsuperscript{245} Furthermore, OPPA will provide better online privacy protections for consumers, better commercial opportunities for businesses who

\begin{footnotes}
\item[232] See Gaudin, supra note 136 (indicating that passage of OPPA would provide necessary support to the lagging high-tech industry by promoting consumer confidence).
\item[233] Letter from Sheila F. Anthony, supra note 166 (highlighting the key provisions of OPPA, which incorporate notice, consent, access, and security).
\item[234] See Thibodeau, supra note 231.
\item[235] See Muris, supra note 11 (discussing the FTC’s privacy initiatives for 2002).
\item[236] See Gaudin, supra note 136.
\item[237] See id.
\item[238] See S. 2201, § 103; see also OPPA Hearing, supra note 217.
\item[239] See Committee Approves Online Personal Privacy Act, S. 2201, supra note 136.
\item[240] See id.
\item[241] See id.
\item[242] See id.
\item[243] See OPPA Hearing, supra note 217.
\item[244] See id.
\item[245] See id.
\end{footnotes}
respond to consumer privacy concerns, and a better future for Americans who will embrace the Internet rather than fear it. 246

IV. CONCLUSION

The benefits of the Internet are astounding, but the associated privacy risks are worrisome. In the era of Internet convenience, one of the greatest challenges is to maintain a sense of privacy. Two current proposals for protecting consumer online privacy, the Online Personal Privacy Act and the Consumer Privacy Protection Act, offer opportunities to advance privacy laws in the United States. Due to its balanced approach to Internet privacy regulation, the Online Personal Privacy Act is the stronger proposal of the two. OPPA seeks to ensure that the right to privacy will endure as new commercial opportunities develop and new technologies emerge.

246. See id.