Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet

SUSAN E. GINDIN

TABLE OF CONTENTS

I. INTRODUCTION ................................................. 1154

II. JUSTICE BRANDEIS REVISITED: HOW PRIVACY MAY BE
    INVADED ELECTRONICALLY ................................. 1156
   A. Personal Information Available Online ................. 1156
   B. Online Privacy ............................................ 1164
      1. E-Mail .................................................. 1164
         a. Workplace E-Mail .................................... 1165
         b. Unsolicited Commercial E-Mail ...................... 1167
      2. Search Engines .......................................... 1169
      4. Online Commerce ........................................ 1172
   C. Government Record-Keeping ................................ 1172

III. PRIVACY PROTECTION TOOLS & PROCEDURES .................. 1174
    A. Self-Help: Online Privacy Protection Tools .......... 1174
    B. Self-Regulation: Information Industry Procedures .... 1179

IV. ENTER THE LAW: PRIVACY RIGHTS IN PERSONAL INFORMATION .... 1184
    A. Constitutional Protections .............................. 1185
       1. Fourth Amendment Protections ....................... 1185
       2. Informational Privacy and Whalen v. Roe ............ 1186
       3. First Amendment Considerations .................... 1187

* Practitioner, Littleton, Colorado; B.A., UCLA; M.S., Drexel University College of Information Science & Technology; J.D., State University of New York at Buffalo. The author thanks the members of her family and Jonathan A. David for their assistance.
I. INTRODUCTION

Subtler and more far-reaching means of invading privacy have become available. . . . Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.\(^1\)

The computer and the modem have fulfilled Justice Brandeis' 1928 prophesy in his landmark dissent in *Olmstead v. United States*. Our private lives are now exposed by the electronic retrieval and publication of personal information. While Justice Brandeis was primarily concerned about governmental intrusion into our private lives, his prophesy and his description of the right to privacy as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men," should apply equally to such intrusion by non-governmental entities.\(^2\) The computer and modem\(^3\) provide both an

---

2. *Id.* at 478 (Brandeis, J., dissenting). Indeed, a "reasonable expectation of privacy" standard is used in the civil privacy arena as well as in the Fourth Amendment context. See, e.g., the workplace e-mail privacy cases discussed *infra* Part IV.E.1. See also PRIVACY WORKING GROUP, INFORMATION POLICY COMMITTEE, INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION, § I.A.3
economical and efficient means of finding needed information. Yet as increasing amounts of personal information are collected and revealed electronically, there is growing concern over the resulting loss of privacy.

In this article, I will discuss (1) how privacy may be invaded electronically; (2) the tools and procedures that are available to help protect individual privacy; (3) the state of the law regarding the rights of individuals to control the disclosure of their personal information; and (4) proposed fair information practices guidelines. As will be discussed, a comprehensive federal policy is needed which will guarantee individuals the right to control the collection and distribution of their personal information. A vital component of this policy would be an informational privacy protection statute which incorporates the basic tenets of fair information practices: the right to limit data collection, data transfers, and secondary uses; the right to access one's personal data and to make corrections; the right to have one's personal data maintained securely; and the right to be informed of data collection and transfer. Such protections will enable individuals to enjoy more fully the many opportunities available throughout cyberspace.
II. **JUSTICE BRANDEIS REVISITED: HOW PRIVACY MAY BE INVADED ELECTRONICALLY**

An individual’s privacy may be invaded electronically in several ways: first, by the significant amount of personal information which is available in online databases; second, by the transactional information collected as the individual participates in online activities; and third, by the massive computerized databases which are maintained by federal, state, and local governments, that may be subject to security breaches.

**A. Personal Information Available Online**

An individual’s privacy may be invaded by the publication of personal information online. A significant amount of personal information is available on the Internet, particularly on the World Wide Web. For example, *Database America* which is a nationwide residential and business telephone directory, includes data on about 165 million households. In addition, *Database America* includes reverse telephone number search capabilities. *Four11: Internet White Pages* provides e-mail addresses as well as telephone numbers and addresses. *Map Blast!* provides area maps which pinpoint requested addresses.

Much of the information provided on the Internet without charge is directory-type information, not traditionally considered private (and in fact, usually recognized as essential for communication), and is therefore not objectionable to most people. However, some of the fee-based Internet sites raise substantial concerns. For example, Information America’s *KnowX*, which is a comprehensive source of public record information, includes aircraft and watercraft ownership, death records, bankruptcy, lawsuit, lien, and judgment information regarding individuals. On *KnowX*, basic information is free; detailed information,
including property records and similar information, is available for a per­
record fee.15

Even more detailed, and often more objectionable, personal informa­
tion is available on commercial online services which are marketed to
legal and business professionals, and journalists. These include
Autotrack, CDB Infotek, Information America, IRSC, LEXIS-NEXIS,
and U.S. Datalink. The personal information available through these
services varies depending on the database, but generally includes name,
address, telephone number, and may include Social Security information,
birthdate, as well as the names and birthdates of other people living at
the same address. Some databases provide real estate records including
data on neighboring properties, approximate household income, plane
and boat ownership, motor vehicle records, voter registration records,
law suits, liens and judgments, criminal records, and credit informa­
tion.16

The commercial online services purchase the personal information they
publish from various sources. Much of the information is obtained from
one of the three credit reporting companies: Equifax, Experian (formerly
TRW), and Trans Union. The credit reporting companies sell the “credit
header” portion of credit histories to commercial online services, as well
as to marketers and other users of personal information. The credit
header data includes name, address, former addresses, telephone number
(sometimes including unlisted numbers), Social Security number, and
birthdate. The online services also purchase the personal information
they publish from information resellers, such as Metromail, which
compile data using census bureau statistics and various sources of
marketing information, including warranty card returns and requests for
product samples and discount coupons. Another source of personal

15. For additional information on people-finding tools available on the Internet, see
<http://www.virtualchase.com/gplla/nov1596.html> (including Foreign Country People
Finding Sites); and PRIVACY RIGHTS CLEARINGHOUSE, *People Finding Tools* (1996)
(visited Sept. 14, 1997) <http://www.privacyrights.org/ar/peoptool.html>. See also The
links to various sources of personal information).

16. See BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REPORT TO
THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING
INFORMATION AND FINANCIAL FRAUD app. C (last modified Mar. 1997)
<http://www.bog.frb.fed.us/boarddocs/RptCongress/privacy.pdf> (presenting samples of
personal information available online).
information is the government. Public records, such as real estate records, are purchased directly from the responsible government agency.  

A great deal of personal information is also revealed in electronic medical records, which are often linked to health records stored in various locations. In addition to being available to doctors and hospitals, most patient records are available to health insurers, pharmacists, state health organizations and researchers. Sometimes these records are also available to employers, life insurance companies, marketing firms, pharmaceutical companies and others.  

The wide availability of personal information online is beneficial in many ways. The Internet site Switchboard, a nationwide residential and business directory, includes heartwarming stories of long-lost friends and relatives being reunited through Switchboard. The commercial online services, such as America Online and CompuServe, relate similar stories of reunions accomplished through the use of their services. Similarly, the lower medical costs (which result from elimination of duplicate testing procedures) is just one of the benefits of computerized medical records. From the viewpoint of a business professional trying to locate critical witnesses or parties to a lawsuit in an online people finder search, the online availability of this information is equally beneficial.

However, this wide availability also raises concerns over the potential misuse of confidential or inaccurate information. Inaccurate

---

17. Telephone Interview with Steve Emmert, Corporate Counsel, LEXIS-NEXIS (Sept. 1996).

18. See Warren E. Leary, Panel Cites Lack of Security on Medical Records, N.Y. TIMES, Mar. 6, 1997, at A1. In March 1997, a National Research Council panel reported that because of widespread use of computerized medical records, security measures should be instituted to increase their privacy and security. Id. In releasing the report, the chairman of the panel, Dr. Paul D. Clayton, said “[m]ost patients would be surprised at the number of organizations that receive information about their health record.” Id. The panel cited the 1996 Health Insurance Portability and Accountability Act, which calls for assignment of “universal patient identifiers” which would link medical records nationwide, as an example of a procedure which provides many benefits, such as assuring consistent care, but which has the potential for serious abuse. Id. at B11.


20. Leary, supra n.18, at A13.

information can result in the denial of credit or government benefits.\(^{22}\) Misuse of confidential information, such as an individual’s Social Security number and other identifying data, can also have severe consequences.\(^{23}\) As commentators suggest, the profile of an individual,

---

\(^{22}\) Almost the entire town of Norwich, Vermont experienced credit problems after a credit bureau employee erroneously listed everyone who had paid their taxes as delinquent taxpayers. **Ellen Alderman & Caroline Kennedy, The Right to Privacy** 326 (1995).

\(^{23}\) For instance, in 1992, a man used the Social Security number of Joe Gutierrez, a retired Air Force chief master sergeant, to open twenty fraudulent accounts. In 1997, Mr. Gutierrez was still being hounded by creditors and their collection agencies. Senator Dianne Feinstein referred to Mr. Gutierrez’ interview with the **San Diego Union Tribune** in her statement introducing the Personal Information Privacy Act of 1997 (S. 600). 143 CONG. REC. S3292 (daily ed. April 16, 1997) (statement of Sen. Feinstein).

Terry Dean Rogan was another victim of identity theft. After Rogan lost his wallet, which contained his driver’s license and credit cards, an impersonator committed two murders and two robberies. Rogan was arrested as a result of a warrant placed in the National Crime Information Center (NCIC) database. Although Rogan attempted to have the NCIC record corrected as soon as he discovered the problem, he was arrested four more times. Ultimately, Rogan sued the Los Angeles police department and was
which can be compiled using information stored in databases, "could be
so complete that it will be like having another self living in a parallel
dimension; it is a self you cannot see, but one that affects your life just
the same."24 Another commentator noted that "once the persona is
recorded it achieves more credence than the individual."25 One victim
of an impersonator (who violated numerous criminal and civil laws in
the name of the victim) was advised that the easiest solution to the
problem of someone using his identity, would be for him to change his
own name and Social Security number.26

In response to privacy concerns, many database providers have
eliminated sensitive information from their databases. In 1996, Yahoo
eliminated the reverse telephone number search from the People Search
site.27 In 1991, in response to consumer complaints, Lotus abandoned
its plans to sell "Marketplace: Households," a database containing
names, addresses and marketing information on 120 million U.S.
residents.28 In 1997, shortly after the Social Security Administration
(SSA) launched its Interactive PEBES (Personal Earnings and Benefit
Estimate Statement) service on the Internet,29 the SSA suspended the
service in response to privacy concerns, pending further assurances that
the online disclosure of PEBES information would not be compromised
by security breaches.30

The Privacy Rights Clearinghouse, which maintains a hotline to assist with privacy
concerns, reported that identity theft, "the fraudulent use of an individual's identifying
data to take over existing credit accounts or apply for new credit accounts and to make
purchases of goods and services in the individual's name," was the "number one topic
of concern" on the PRC hotline in 1996. Beth Givens, PRIVACY RIGHTS CLEARING-
HOUSE, Comments on the Availability of Sensitive Information About Consumers and Its
Possible Use for Financial Fraud, in BOARD OF GOVERNORS OF THE FEDERAL RESERVE
SYSTEM DOC. NO. R-0953 (Jan. 30, 1997) (comments on "credit header" information as
well as the widespread availability of Social Security numbers, made upon request for
24. ALDERMAN & KENNEDY, supra note 22, at 326.
25. Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as
question of what happened to searching by telephone number, the Web site states: "We
have elected to discontinue the reverse lookup feature because of privacy concerns that
have been raised by users."
28. Lawrence M. Fisher, New Data Base Ended By Lotus and Equifax, N.Y.
In 1996, LEXIS-NEXIS introduced P-TRAK, which provides up to three addresses, as well as aliases, maiden names, and birthdates for over 300 million people, including Social Security numbers (at the time of its introduction). There was considerable public uproar and discussion in the media and on Internet discussion groups. In response to concerns expressed about the potential misuse of Social Security numbers, LEXIS-NEXIS removed the display of Social Security information from the records within two weeks after P-TRAK’s introduction (although records can still be searched using the Social Security number). Public concern about P-TRAK arose again a few months later when postings appeared on numerous Internet discussion groups incorrectly stating that P-TRAK contains personal financial and medical information, as well as displays of Social Security numbers. This misinformation spread quickly to different Internet discussion groups and eventually to corporate e-mail. LEXIS/NEXIS Customer Service was soon inundated with calls from people requesting removal of personal data from P-TRAK. In addition, Congress and the Federal Trade Commission (FTC) were inundated with P-TRAK complaints from constituents. LEXIS/NEXIS responded by providing various means for individuals to remove personal information from the P-TRAK database. The FTC responded by urging Congress to amend the reporting of consumer information provisions of the Fair Credit Reporting Act.\(^{31}\)

There are currently no laws regulating the publication of personal information in online databases. Unless steps are taken to regulate the

PEBES reports, which detail an individual’s Social Security tax contribution and an estimate of retirement and disability benefits, are available by mail upon written request containing full name, Social Security number, date of birth, place of birth, and mother’s maiden name. Access to an online report required submission of the same information, but the Social Security Administration was concerned about the security and confidentiality of the online system. \(\text{Id.}\)

\(^{31}\) See discussion regarding the Fair Credit Reporting Act, infra Part IV.D.5.

LEXIS/NEXIS obtains the data for P-TRAK from the credit reporting agency Trans Union. The Federal Trade Commission had previously decided that credit header information is not covered by the Fair Credit Reporting Act, and therefore not subject to the FCRA restrictions governing the distribution of credit information. As a result of consumer complaints regarding P-TRAK, the FTC has reconsidered this position. See Laurie J. Flynn, Lexis-Nexis Flap Prompts Push for Privacy Rights, N.Y. TIMES CYBERTIMES (Oct. 13, 1996) <http://www.nytimes.com/library/cyber/week/1013nexis.html>; Cindy L. Chick, LEXIS/NEXIS Held Hostage By the Internet: The P-Trak Debacle, SEARCHER MAG. (Nov./Dec. 1996) <http://www.llrx.com/features/ptrak.htm>.
access to personal information online, the availability of this information will continue to increase. Several factors have converged during the second half of the twentieth century to cause this increased availability of personal information. One factor is that society has become dependent on information. Businesses, government, and some individuals need information to function effectively. Personal information is used by federal, state, and local governments for various purposes, including collection of taxes, allocation of government benefits, and law enforcement. Personal information is required by businesses to make hiring and credit-granting decisions and for the successful marketing of products.

Commentators say we have entered an information age, resulting from the transformation of society's economic base from industry to information. One commentator noted that "[i]nformation has taken on a new character . . . it has passed from being an instrument through which we acquire and manage other assets to being a primary asset itself." In 1997, information was the product of over 550 private companies, which includes credit reporting agencies, interactive online services, database producers, and financial information services, with annual revenues somewhere in the billions. The sale of information is also...
a source of substantial revenue for government agencies. The information industry has been growing dramatically every year, and shows no signs of slowing down.

Another factor contributing to the wide availability of personal information online is the government’s initiative to make government records readily available to the public. Citizen access to government information was assured by the 1966 enactment of the Freedom of Information Act (FOIA), followed by the enactment of similar state statutes, which codified long-standing philosophies that the free flow of information between the government and the public is essential to a democratic society.

The government’s initiative took on new significance with the development of the Internet and other online databases which offered a means for widespread dissemination of government records. In 1993, the Office of Management and Budget established an Information Management Policy that included the online dissemination of government records. A number of government agencies have made their


Beginning in 1997, the dissemination of state motor vehicle records will be subject to some restrictions under the Driver’s Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (1994).

38. John Sculley, former CEO of Apple Computers, has estimated that by the year 2000, the information industry, including computer, telecommunications, television, entertainment and news industries, will be worth $3.5 trillion. Prepared Statement by AMP Incorporated; Presented by Henry Line, Director, Global Product Standards, to the Subcomm. on Tech., Env’t, and Aviation Hearing of the House Comm. on Science, Space & Tech., FED. NEWS SERV. Sept 22, 1994 (available in LEXIS-NEXIS, News Library, Allnws File).


40. BRANSCOMB, supra note 33, at 163-64 (quoting President James Madison: “A popular government, without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own Governors, must arm themselves with the power knowledge gives.” (1822)).

records available electronically via commercial online services or via the Internet. A third factor contributing to the widespread availability of personal information online is the development of computer and telecommunication technologies, including the Internet. These technologies have enabled the information industry to flourish by providing the means for government and private industry to collect and manage vast amounts of data, and to transmit that data around the world. Because information can be obtained and transmitted so quickly, heightened expectations regarding information availability are created. It is likely that those in need of personal information will demand even more online access.

B. Online Privacy

Computer technology also provides the means for collecting personal information which is incident to the use of online services and the Internet. The Internet has the capacity to be the most effective data-collector in existence. Concerns about the collection and potential misuse of personal information are multiplying as new ways of electronically collecting personal information emerge. An online user's privacy may also be invaded by his use of electronic mail, online services, and the Internet.

I. E-mail

In 1994, 776 billion electronic-mail (e-mail) messages passed through U.S. based computer networks. Projections are for 2.6 trillion e-mail messages to pass through U.S. networks in 1997, and for 6.6 trillion e-mail messages to pass through U.S. networks in 2000.
One’s privacy may be invaded when sending e-mail, which is notably insecure. The Internet functions by sending data from computer to computer in packets until the data reaches its destination. While traveling to the intended recipient, third parties have many opportunities to intercept the data.

a. Workplace E-mail

One’s privacy may also be invaded in the workplace:

It’s a situation that arises a million times a day in offices around the world. An employee has something personal to tell a co-worker. Rather than pick up the phone or wander down the hall, he or she simply types a message on a desktop computer terminal and sends it as electronic mail. The assumption is that anything sent by E-mail is private. That assumption, unfortunately, is wrong.

In a survey of 500 executives by the Society for Human Resources Management, 36% said they looked at employee e-mail. A similar survey conducted by *MacWorld* showed that nearly two-thirds of those employers who monitored their employees’ e-mail, electronic work files, network messages, or voice mail, did so without warning the employees.

Employers monitor employee e-mail for a number of reasons. Some businesses conduct employee e-mail, telephone, and keystroke monitoring routinely to assist in the training of new employees.

47. See, e.g., Richard Behar, *Who’s Reading Your E-Mail?*, *Fortune*, Feb. 3, 1997, at 57, 58 (quoting Bruce Schneier, *E-mail Security: How to Keep Your Electronic Messages Private* (1995): “The only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location—and I’m not completely confident of that one either.”).


52. In response to the need of employers to monitor employee electronic communications, several companies now sell “Internet Management Software.” This software, which analyzes Internet and intranet usage, can be used to monitor the content of employee electronic communications. See, e.g., Sequel Technology (visited Sept. 10, 1997) <http://www.sequeltech.com>. 
Others monitor e-mail because of concerns about trade secret misappropriation\textsuperscript{53} or liability for employee defamation, harassment, copyright infringement, as well as other electronic misdeeds by employees.\textsuperscript{54}

Many employees feel that an employer monitoring their e-mail is an invasion of privacy. As a result, there has been a significant amount of litigation over workplace e-mail privacy.\textsuperscript{55} Although the courts have so far ruled that the employees had no reasonable expectation of privacy in their workplace e-mail, this issue will surely engender additional litigation.

E-mail messages can usually be retrieved from a variety of locations, including the network, local hard drives, and backup tapes, even if they have been deleted. E-mail sent or received on an employer's computer

\textsuperscript{53} See, e.g., Borland Int'l, Inc. v. Eubanks, No. 123059 (Cal. Super. Ct., Santa Cruz County, 1992) (charging trade secret misappropriation because a recently resigned executive vice president, Eugene Wang, who had joined a competing company had sent sensitive Borland information via e-mail to the competing company's president, Gordon Eubanks). See also People v. Eubanks, 927 P.2d 310, 312 n.2 (Cal. 1996) (charging Wang and Eubanks with trade secret theft but subsequently dismissing the case, after oral argument, at the request of the county district attorney); Borland Secrets Suit Ends, N.Y. TIMES Feb. 17, 1997, at 47 (stating that the civil suit was settled by the parties in April 1997).

\textsuperscript{54} In 1995, four female employees of Chevron sued the company for sexually harassing e-mail. Amie M. Soden, Protect Your Corporation from E-Mail Litigation: Privacy, Copyright Issues Should Be Addressed in Policy, CORP. LEGAL TIMES, May 1995, at 19. Although Chevron denied liability, the company settled for $2.2 million plus legal fees and costs. Id. In 1997, some black employees of Morgan Stanley, R.R. Donnelley & Sons, and Citibank brought suit against their respective employers charging the companies with racial discrimination for allowing the distribution of bigoted e-mail by other employees. Michelle Singletary, Loose Lips an E-Mail Hazard, WASH. POST, Apr. 6, 1997, at F12.


system is also discoverable and is subject to review by law enforcement officials in criminal investigations.

In light of the many potential difficulties which can arise with regard to employee e-mail use, many commentators urge that employers prepare carefully drafted policies regarding employee Internet and e-mail use.

b. Unsolicited Commercial E-mail

One's privacy may be invaded by unsolicited commercial e-mail, also known as junk e-mail or "spam." Junk e-mail is generated by Internet marketers, which compile their mailing lists using the header information (e-mail address, name, service provider) provided with Internet postings, as well as information provided by users when registering to use certain Web sites.

Junk e-mail can also be intrusive. However, not all unsolicited commercial e-mail is objectionable; some is informative and useful. One survey by an Internet service provider revealed that 70 percent of its users are not bothered by receiving unsolicited commercial e-mail as long as it is tailored to their interests.

However, the bulk mailing of unsolicited e-mail has become a serious concern for online service providers. These mailings hinder their ability to process legitimate subscriber mail and harm their relationships with subscribers. Some service providers have resorted to litigation.

57. For discussion of considerations in drafting company e-mail and Internet use policies, see Casser, supra note 54; Cyberspace Law Institute, Company Email Policy (visited Sept. 11, 1997) <http://www.cif.org/emailpolicy/top.htm>; Dichter & Burkhardt, supra note 55; Ellis & Chase, supra note 55; Marshall & Ross, supra note 54; Donald S. Skupsky, Discovery and Destruction of E-mail, THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES, Ch. 5 (1996) <http://cla.org/RuhBook/chp5.htm> (discussing policy considerations in light of Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993) (holding that federal government e-mail is a record as defined by the Federal Records Act, unless excluded under appropriate procedures)).
59. In Spring 1997, for instance, a bulk e-mailing to customers of Netcom, the sixth-largest Internet service provider, shut down Netcom for more than a day. Id.
60. In addition to the difficulty for subscribers in connecting to the service because the junk e-mail clogs the system, some e-mailers alter the messages' header information so that it appears the message came from the service.
directed primarily at the largest commercial e-mailer, Cyber Promotions, which sends out 15-20 million unsolicited e-mail messages a day.62

Some legislation has been proposed which would regulate unsolicited e-mail.63 Four federal bills were introduced in 1997,64 the state of Nevada enacted legislation regulating unsolicited e-mail in July 1997,65 and other states have proposed legislation.66

In addition, numerous print and Web articles provide suggestions for reducing junk e-mail.67 Suggestions range from asking the advertiser not to send additional junk e-mail to using an Internet address filter that blocks communications from known commercial e-mail sites. Other potential solutions allow individuals to "opt-out" of e-mailings. Apex Global Internet Services (AGIS),68 an Internet service provider which hosts commercial e-mailers, announced a plan in April 1997 to create a master list of users who don't want to receive unsolicited commercial e-mail, and then require any e-mailers who use AGIS' service to remove those names from their e-mailing lists.69 America Online70 has devised a system in which subscribers have the opportunity to choose

61. See discussion infra Part IV.E.2.
62. Simons, supra note 58, at 55.
64. These include: Netizen's Protection Act of 1997, H.R. 1748, 105th Cong., 1st Sess. (1997), which was introduced by Representative Christopher Smith of New Jersey; Unsolicited Commercial Electronic Mail Choice Act of 1997, S. 771, 105th Cong., 1st Sess. (1997), which was introduced by Senator Frank H. Murkowski of Alaska; Electronic Mailbox Protection Act of 1997, S. 875, 105th Cong., 1st Sess. (1997), which was introduced by Senator Robert Torricelli of New Jersey; Data Privacy Act of 1997, H.R. 2368, 105th Cong., 1st Sess. (1997), which was introduced by Representative Billy Tauzin of Louisiana. See also discussions regarding the proposed legislation, and discussions as to whether the Communications Act section banning unsolicited faxes already prohibits unsolicited e-mail, on the NET-LAWYERS listserv from May 22, 1997 (archived at <http://eva.dc.lsoft.com/Archives/net-lawyers.html>).
whether or not they want to receive e-mail from known commercial e-mailers.71

2. Search Engines

An Internet user's privacy can also be invaded by search engines.72 Search engines use "robots" to continually peruse the World Wide Web and Usenet newsgroups73 for additions to their databases which attempt to index every word. DEJA NEWS,74 for instance, prides itself on indexing all Usenet postings, and keeping them "until the end of time."75

Search engines raise privacy concerns because of their capacity to capture and preserve every message communicated in Usenet postings and archived listserv76 postings. Although a Usenet group or listserv may appear to be merely a collegial and confidential exchange of information, postings often achieve Internet-wide distribution when they are archived and/or included in the search engine databases.

An individual's postings to Internet discussion groups and his or her World Wide Web site can be found through search engines. Thus, those participating on the Internet should be cautious about what they write.77

---

73. Usenet newsgroups are electronic discussion groups that are similar to bulletin boards where participants use a common location to read and post messages. See DEJA NEWS (visited Sept. 13, 1997) <http://www.dejanews.com/info/idg.shtml> (providing a detailed explanation of Usenet).
75. See DEJA NEWS, supra note 74.
76. A listserv is a type of automatic mailing list that permits discussion of particular topics via e-mail communication. A listserv subscriber contributes messages on the topic to the listserv that are forwarded to anyone who has subscribed to the list.
77. DejaNews cautions:
Be Careful What You Say About Others. Please remember—you read netnews; so do as many as 3,000,000 [updated to 22,000,000] other people. This group quite possibly includes your boss, your friend's boss, your girl friend's brother's best friend and one of your father's beer buddies. Information posted on the net can come back to haunt you or the person you are talking about.

An Internet user's privacy may be invaded by certain features used by the online services and World Wide Web site operators to maintain and improve their service. Some Web sites collect "cookies." A cookie is information about the Web site visit, which the Web browser receives from the Web site, and then stores on the visitor's hard drive. The Web site then "reads" the information each time the user visits the site. This information includes the visitor's Internet service provider, the kind of computer and software used, the Web site linked from, as well as which files were accessed and the amount of time spent on each page. The information is used to track visits to the Web site to learn what visitors like and dislike about the site, and to personalize the site so that options the user selects at the first visit can be used automatically for each successive visit.

As such, the information collected does not usually identify a specific individual. However, when combined with on-site registration data, which the Internet user provides when visiting some sites, cookie data may be used to build a profile of the specific Internet user. Many Web sites require on-site registration, including name, address, e-mail address, and sometimes interests, in order to obtain access or certain benefits.

Internet service providers can also track a user's navigation on the Internet using electronic records of user activity, also referred to as "clickstream" data. Online service providers track navigational patterns on their services to make improvements. In its Terms of Service, America Online explains that it records users' "navigational and transactional" information to "understand our members' reactions to..."
menu items, content, services and merchandise offered through AOL and to customize AOL based on the interests of our Members." 82

Of particular concern is the on-site registration information requested on Web sites directed at children. 83 Many Web sites directed at children solicit personal information about the child and child’s family, often in exchange for an opportunity to participate in a contest or in the activities offered on the site. 84 The Web site providers use this monitoring information for various purposes. The information is used primarily for marketing, 85 but is also used to improve the Web site. 86 One provider of a Web site for children uses the identity information it obtains to prohibit future access to the Web site for visitors who have behaved inappropriately at prior visits. 87

The information collected from Web site visits reveals much about the user. Even without providing personal information when registering to use a site, a user’s interests can be inferred based on Web site or online service use. Accordingly, there is concern that this information will be misused by marketers and others.

The autonomous software agents that are being developed at the MIT Media Laboratory and elsewhere engender similar concerns due to the personal information these software agents can collect. Software agents, which are being developed to deal with information overload problems, operate like librarians—after determining the user’s interests, they suggest additional resources that might be of interest. MIT’s Web browser agent, Letizia, determines the user’s interests by “observing” the Web sites and pages accessed by the user, and then recommends additional resources by previewing immediately accessible links. In addition to the Web browser agent, MIT has developed agents that will recommend music and books, and is working on others, including a

84. Id. For example, on the Batman Forever Web site, the cartoon character Batman asks children to enter information about their families. Id. at IV.B. n.13.
85. Id. at IV.B.1.
86. Id.
87. Id. at IV.B.1 n.23.
“Yenta-Matchmaking” agent that will introduce people who share similar interests.\textsuperscript{88}

4. Online Commerce

Online commerce via the Internet has enormous potential,\textsuperscript{89} but raises additional privacy concerns. Activities such as online purchases and banking necessitate the disclosure of so much personal information, including name, address, and credit card or account information, that they require special security procedures. Use of encryption\textsuperscript{90} is necessary, and additional security measures, such as the use of digital signatures\textsuperscript{91} are recommended.\textsuperscript{92}

C. Government Record-Keeping

One’s privacy may also be invaded by the collection, maintenance, and dissemination of government records. For efficiency and economy, government agencies have automated (or are in the process of automating) their records.\textsuperscript{93} Some government agencies are providing agency records on their Web sites.\textsuperscript{94} Although these agencies have been


\textsuperscript{90}See encryption discussion infra Part III.A.

\textsuperscript{91}Lori Jean G. Oei, Digital Signatures, in ONLINE LAW: THE SPA’S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET 41-61 (1996).

\textsuperscript{92}See Thomas J. Smedinghoff, Online Payment Options, in ONLINE LAW: THE SPA’S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET 103-19 (1996).

\textsuperscript{93}The Internal Revenue Service has been criticized for its significant problems in implementing its $23 billion “Tax System Modernization” (TSM) program which was to have upgraded its computer and information systems by the year 2008. See John Broder, Are I.R.S. Computers Deductible? How an Agency Was Left Behind on the Road Ahead, N.Y. TIMES, Feb. 10, 1997, at D1. See also E. Maria Grace, Privacy vs. Convenience: The Benefits and Drawbacks of Tax System Modernization, 47 FED. COMM. L.J. 409 (1994) <http://www.law.indiana.edu/fclj/v47/no2/grace.html> (discussing Tax System Modernization Program).

applauded for making this data available on the Internet for free,95 the
security of the information is an important concern.96

Certain records such as tax, social welfare, and criminal history
information, are considered confidential and are only available to
authorized government employees.97 Other records, including property
records, birth, death, and marriage certificates, court records, motor
vehicle and voter registration records of many states, are considered
public records. The online service providers, as well as direct marketers,
obtain much of the personal information they sell from public records.98

Computerization of the records has facilitated intergovernmental
resource-sharing. The FBI’s National Crime Information Center (NCIC)
database, which maintains information on federal, state, and local crime
convictions, is invaluable for state and local, as well as for federal, law
enforcement officials. Also, the federal government’s computer-
matching program permits agencies to compare records for various
reasons, including determining eligibility for benefit programs and
collecting unpaid child support or debts owed the government.99

However, the computerization of government databases raises several
concerns. One concern is the accuracy of the records. Depending on
their nature, they may be sold to online service database providers, used
by credit reporting agencies in creating credit profiles, or used by
another government agency to verify eligibility for certain benefits.

Another concern is the security of government databases, especially
the massive federal databases, including the FBI’s NCIC and the IRS

95. Id.
96. See, e.g., supra notes 29-30, and accompanying text (regarding suspension of
the Social Security Administration’s interactive PEBES Internet service pending
assurances that the data would remain secure); see also OMB Watch, A Delicate
Sites (visited Sept. 15, 1997) <http://ombwatch.org/ombw/priv11.pdf> (reporting that in
a study of the Web sites of seventy federal government agencies, OMB Watch found that
thirty-one of the sites collect information about visitors to their sites; of those thirty-one
sites, only thirty-five percent indicate to users how that information is being used).

97. See generally RAYMOND T. NIMMER, INFORMATION LAW § 8.16 (1996);
PRIVACY RIGHTS CLEARINGHOUSE, Fact Sheet #11: From Cradle to Grave: Government
fs/fs11-pub.html> [hereinafter From Cradle to Grave].

98. States make much money on the sale of this public information. See, e.g.,
supra note 37 (regarding the amount of revenue some states generate from the sale of
its motor vehicle information).

99. See From Cradle to Grave, supra note 97, at 4.
database. Tax return information, which includes not only name, address, occupation, and income, but also family data, financial data, and medical information, provides a nearly-complete personal profile.

Unauthorized access to these government records is a very real concern. A commentator reported that "security risks to federal computers and telecommunications systems are worse than ever. Every day the confidentiality, integrity and availability of government information is being threatened by amateur hackers, [viruses], professional eavesdroppers, power outages, natural disasters and human error." Government agencies are aware of security risks and have taken security measures. However, security breaches continue. Computer hackers have broken into computer systems of the Central Intelligence Agency, Justice Department, National Aeronautics and Space Administration, and the World Wide Web page of the Air Force.

III. PRIVACY PROTECTION TOOLS & PROCEDURES

There are some tools and procedures that offer some protection for individual privacy. Certain tools can be used by individuals to help protect their online privacy, and specific procedures can be used by the information industry to safeguard the privacy of individuals. These tools and procedures have varying degrees of effectiveness, but are essential components for privacy protection.

A. Self-Help: Online Privacy Protection Tools

A variety of privacy protection tools can be used to help protect online privacy. The most popular and effective tool is encryption, which is a procedure which scrambles electronic documents so that they can only be unscrambled using the proper key or keys. One of the most


Amateur hackers, viruses, professional eavesdroppers, power outages, natural disasters, and human error are not the only challenges to the confidentiality of government records. The General Accounting Office reported to Congress that in 1994 and 1995 alone, there were 1,515 known cases of Internal Revenue Service employees “snooping” through taxpayer files. Congress Passes Anti-Browsing Measure, Prompting Calls for More Reform of IRS, 2 BNA’s ELECTRONIC INFO. POLICY & LAW REP. 434-35 (1997). In response, Congress passed legislation in 1997 that would criminalize unauthorized access to taxpayer files by I.R.S. employees. Id.

popular and powerful software encryption programs is PGP (Pretty Good Privacy).102

While encryption is widely recognized as essential for privacy protection and security, it is a controversial topic because the federal government has vigorously attempted to regulate encryption standards and technologies, while software manufacturers and some privacy organizations have attempted to minimize government encryption controls.103 The government is concerned both about national security and that encryption will give criminals the means to frustrate law enforcement efforts. Therefore, the government wants to ensure a means to access encrypted items and to restrict the export of encryption software.104 In 1993, the Clinton administration announced the Clipper Chip Proposal as a solution to the government's need to access encrypted data. This proposal involved the use of a microprocessor chip that would encrypt and decrypt data using a private/public key system, requiring that the private keys be held in escrow by the government to allow the government easy access to encrypted data. This proposal was so widely criticized that the government abandoned the original proposal a year later. In October 1996, the Administration announced a plan for a "worldwide key management infrastructure with the use of key escrow and key recovery [a system allowing individuals to reclaim lost codes] encryption items" in connection with export control regulations.105 Later in 1996, control for the export of encryption software was


transferred from the U.S. State Department’s *U.S. Munitions List* to the Commerce Department’s *Commerce Control List*. The Commerce Department Bureau of Export Administration (BXA) issued interim rules for encryption export regulations.

Three recent federal cases have involved challenges to the constitutionality of encryption software export restrictions. In *Junger v. Daley [Secretary of Commerce]*, filed in August 1996 in the U.S. District Court for the Northern District of Ohio, a law professor, who wishes to publish some encryption programs on his Internet site as part of the course materials for his Computing and the Law course, is seeking to enjoin the government’s enforcement of encryption software export regulations. The other two cases have produced opposite results. In *Bernstein v. U.S. Dept. of State,* the U.S. District Court for the Northern District of California ruled that the export control regulations, which would prevent the plaintiff from distributing his encryption software over the Internet without a license, violate the First Amendment’s free speech guarantee. In contrast, the U.S. District Court for the District of Columbia ruled, in *Karn v. U.S. Department of State,* that the State Department export control regulations do not raise First Amendment issues. The *Karn* court further held that the restrictions consist of foreign policy decisions which are not the province of the courts.

On appeal to the U.S. Court of Appeals for the D.C. Circuit, *Karn* was remanded for reconsideration in light of both the late 1996 transfer of regulatory authority for the export of encryption software from the State Department to the Commerce Department, and the Commerce Department’s issuance of new regulations.

Another privacy protection tool is the use of an anonymous server to send e-mail or access Internet sites anonymously. An anonymous server acts as a middleman between the Internet user and the document the user wants to send or retrieve. The only identifying information available to the site that is contacted is the address of the anonymous server. For example, for Web, FTP, and gopher transactions, Community

110. *Id.* at 1310.
112. *Id.* at 8-10.
114. FTP (File Transfer Protocol) permits an online user to log onto, review, and transfer files to and from another computer.
ConneXion, Inc. (whose motto is: "Because on today's Internet, people do know you're a dog") provides the Anonymizer.\textsuperscript{116} For e-mail and Usenet postings, an anonymous remailer will strip e-mail and Usenet postings of identifying information, and then forward the message to the recipient.\textsuperscript{117}

Anonymity also has its critics.\textsuperscript{118} In 1996, a Georgia statute took effect prohibiting online users from using pseudonyms or communicating anonymously over the Internet.\textsuperscript{119} In response, the A.C.L.U. and the Electronic Frontier Foundation brought suit in September 1996 in the Federal District Court for the Northern District of Georgia, and obtained a preliminary injunction against enforcement of the statute.\textsuperscript{120}

Other procedures can be used to prevent the widespread distribution of Usenet postings and Web pages. If a Web site is not for public use, security measures can be utilized, including passwords, domain name filtering, Internet address filtering, or a firewall\textsuperscript{121} to prevent access by unauthorized users. Also, by using the "Standard for Robot Exclusion," search engine robots will ignore all or designated parts of the Web site.\textsuperscript{122} To avoid having a Usenet posting indexed by a search engine,
"X-no-archive: yes" should be added to the header of the message or made the first line of the message.

In response to concerns about cookies, newer versions of Web browsers, such as Netscape 3.0, have mechanisms which notify the user before a cookie is set. Software has also been developed to assist users in managing cookies.

With regard to children's privacy, there is software available which gives parents the opportunity to monitor, filter, and prevent information disclosure by their children. For instance, Cyber Patrol, which enables parents to prevent access to inappropriate sites, also enables parents to prevent the disclosure of specific previously identified information. In addition, Microsoft's browser, Internet Explorer, and some online services provide parents with blocking options.

Filtering can also be used to reduce unsolicited commercial e-mail. Filters can be used to block e-mail that matches categories, such as sender or subject. Unfortunately, commercial e-mailers frequently alter the message header to disguise the subject and indicate a different sender.

Some companies have devised systems to protect user privacy while satisfying the needs of online marketers to obtain information about current or potential customers. For example, Internet Profiles Corporation (I/PRO), a market research firm, has proposed a universal registration system involving the assignment of codes that would enable users to browse the Web anonymously. Personal information, which users would provide to I/PRO at registration, would be transmitted anonymously as part of the code.

125. See FTC 1996 REPORT, supra note 83, at nn.63-70 and accompanying text.
128. In the Cyber Promotions cases, in which the e-mail marketers created mass e-mailings, a major complaint of the Internet service provider (ISPs) was Cyber Promotions' practice of altering message headers to disguise their true e-mail address, while sometimes indicating that the commercial e-mail originated with the ISP. See discussion infra Part V.E.2.

1178
In May 1997, Internet technology companies, Netscape Communications Corp.,\textsuperscript{132} Firefly Network Inc.,\textsuperscript{133} and VeriSign Inc.,\textsuperscript{134} proposed a similar system as an industry standard. The Open Profiling Standard (OPS) will give users control over the personal information they reveal online while enabling companies to gather personal information for marketing purposes and to personalize Internet services. Under this system, users enter name, address, and other personal information that is useful to marketers and online services (such as age, gender, marital status, and product preferences) into a file which resides on their hard drive. When accessing a Web site that requests personal information, users will have the opportunity to specify which information should be revealed, and whether their personal information can be shared with other Internet sites. The Open Profiling Standard has the support of approximately one hundred companies, including advertisers, consumer Web sites, search engine companies, and software and hardware companies.\textsuperscript{135}

The proposed Open Profiling Standard, and other technological measures developed and implemented by Internet technology companies, are examples of the significant role the information industry can take in assuring individual privacy. The information industry may also play a significant role in assuring individual privacy by self-regulating the procedures used in collecting and disseminating personal information.

\textbf{B. Self-Regulation: Information Industry Procedures}

The procedures used by the information industry in collecting and using personal information determine whether individual privacy is invaded. Many information industry companies have taken steps to ensure that these procedures protect individual privacy.

Information industry organizations have issued industry guidelines for fair information handling, which include privacy protection proce-
In addition, many companies have established privacy protection policies. Some companies have abandoned projects that were objectionable to the public. For example, Lotus abandoned its Marketplace database and LEXIS-NEXIS withdrew Social Security numbers from P-TRAK records.

There is much incentive for information companies to comply with industry guidelines, and to respond to the pressures of the marketplace. Studies have shown that consumers are nervous about electronic privacy and about transacting business via the Internet. As noted by the Interactive Services Association guidelines, online service providers need to safeguard subscribers' privacy or risk losing subscribers:

The first rule of business is to establish the trust of the subscriber. . . . Although there are no laws protecting subscriber information, other than with respect to e-mail, the industry has made the protection of such information a priority.

Online service providers recognize that they have an interest in providing this information.
protection and maintaining the subscriber's trust because if subscribers feel that their information is not protected they will no longer subscribe to the online service. Accordingly, the online service companies have developed these guidelines to establish an industry-wide standard prohibiting the disclosure of individual session activities and setting forth the steps which must be taken before making certain other subscriber information available to third parties. 140

By mid-1997, there was substantial industry and governmental support for self-regulatory measures as the preferred means for protecting Internet privacy. In July 1997, the Clinton Administration expressed its support for the use of self-regulatory measures as the preferred means for protecting Internet privacy by issuing A Framework for Global Electronic Commerce. 141 The Framework generally favors a laissez-faire, market-driven approach to regulating the Internet in an effort to stimulate electronic commerce.

In June 1997, the Federal Trade Commission held a public workshop on consumer information privacy. At this workshop, representatives of the information industry and privacy organizations discussed electronic privacy. 142 Industry representatives strongly urged the use of technological measures and industry self-regulation to safeguard consumer privacy. LEXIS-NEXIS, and seven other information companies which provide personal information, proposed industry guidelines which would ensure the accuracy and security of the information provided, limit the availability of non-public information, and educate consumers about the practices of the information companies. 143 In addition, during the Federal Trade Commission workshop, the Open Profiling Standard proposed a few weeks earlier by Netscape Communications (and other

Internet technology companies) gained additional support from other information industry companies.\textsuperscript{144}

Also in June 1997, the U.S. Commerce Department’s National Telecommunications and Information Administration published a report, \textit{Privacy and Self-Regulation in the Information Age}.\textsuperscript{145} In this report, legal scholars, economists, and numerous representatives of the information industry discussed the effectiveness and legality of industry self-regulation. Various approaches to privacy protection were discussed within the context of industry self-regulation. One contributor proposed using a contractual approach to privacy protection. Individual privacy rights would be established through contracts made with data collection companies.\textsuperscript{146} Other contributors proposed using a property approach, through which individuals would be paid for use of their personal information by the data collectors.\textsuperscript{147} A number of representatives of large information companies also detailed their companies’ existing privacy policies.

Nonetheless, the self-regulatory approach to informational privacy protection in the U.S. may be thwarted by data protection laws in the European Union. The European Union’s comprehensive data protection directive, which takes effect in October 1998, both requires member countries to enact statutes which protect individual rights to privacy with respect to the processing of personal data, and requires that personal information may only be transmitted outside the European Union to a country which ensures an adequate level of protection for the subject of the data.\textsuperscript{148} The directive will affect all U.S. entities conducting transactions which involve personal data transfers with European entities.

\begin{itemize}
\item \textsuperscript{144} Steve Lohr, \textit{MicroSoft Joins Netscape on Software Privacy}, \textit{N.Y. TIMES}, June 12, 1997, at D4.
\item \textsuperscript{145} (Visited Jan. 23, 1998) \url{http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm}.
\item \textsuperscript{148} Directive 95/46, 1995 O.J. (L281) 31 (requiring that the member country statutes provide individuals with the right to advance notice of a data collector’s intent to collect and use their personal data, the right to access and correct data collected about them, and the right to object to certain data transfers, as well as require that data collectors both maintain the security and confidentiality of personal data, and provide judicial remedies for violations).
\end{itemize}
In a policy paper issued in June 1997, the European Commission indicated that "adequate protection" should be determined by examining both the content of the country's privacy rules as well as the procedural mechanisms in place to ensure the effectiveness of these rules. The European Commission further indicated that the current U.S. privacy protection measures are unlikely to meet the directive's "adequate protection" requirements. Thus, without legislation or some other formal mechanism to enforce informational privacy rights, personal data transfers from the European Union to the U.S. may be prohibited after the European Union data protection directive takes effect in October 1998. Such restrictions would have a momentous impact on electronic commerce, especially in light of the directive's all-encompassing approach to data protection. The policy paper specifically mentions credit card payments over the Internet, as well as "transfers involving the collection of data in a particularly covert or clandestine manner (e.g. Internet cookies)" as examples of data transfers which would receive particular scrutiny in terms of "adequate protection."

The European Community clearly questions the adequacy of informational privacy protection in the United States. Although there is much support in the U.S. for self-regulatory measures and technological privacy innovations, substantial doubt remains as to whether these measures can be completely effective without some type of enforcement mechanism. Unless there are sanctions available for violations of

150. Id.
151. Some personal data transfers to U.S. entities may still be allowed. For certain situations, the Directive's Article 26 allows data transfers to a third country which does not meet the adequate protection standards set out in the Directive's Article 25. For instance, personal data transfers will be permitted where the data subject has consented. Personal data transfers may also be permitted, on an ad hoc basis, where the entity receiving the data has taken appropriate steps to ensure individual privacy protection. Article 26(2) indicates that appropriate contractual clauses may constitute the requisite privacy protection guarantees. See also Susan E. Gindin, Everyone Knows You're a Dog: The EU Data Protection Directive and Personal Data, J. INTERNET L., Mar. 1998; (visited Mar. 8, 1998) <http://www.info-law.com/eupriv.html>.
152. EUROPEAN COMMISSION, supra note 149.
153. See, e.g., FTC 1996 REPORT, supra note 83, at III. (Enhancing Consumer Privacy Online), <http://www.ftc.gov/bcp/conline/pubs/privacy/privacy4.htm>. See also Letter from Representatives of the Center for Media Education, Privacy Rights Clearinghouse, Privacy Times, Electronic Frontier Foundation, Consumer Federation of
industry guidelines, some information companies may be inclined to ignore industry guidelines or to minimize their significance in their quests for profits.\textsuperscript{154}

The self-regulatory measures of the U.S. information industry should be encouraged even if these measures are deemed insufficient in safeguarding the informational privacy of individuals. These safeguards can be effective if consistently followed and offer the significant benefit of addressing and resolving issues which arise more quickly than through the legislative process or other methods of redress.

IV. ENTER THE LAW: PRIVACY RIGHTS IN PERSONAL INFORMATION

In the United States, there is no comprehensive law guaranteeing privacy rights in personal information. Contrast this to Europe, where the European Union's comprehensive data protection directive takes effect in October 1998.\textsuperscript{155} In the United States, informational privacy protections are provided by an assortment of federal and state constitutional law, statutory provisions, and judicially determined case law.

\begin{itemize}
\item <http://www.epic.org/privacy/databases/ftc_letter_0797.html> (challenging the Federal Trade Commission's preliminary findings of the Public Workshop on Consumer Privacy (i.e., the FTC's assessment that the American public favors the employment of self-regulatory measures and prefers technological approaches as the best means for protecting children's online privacy) and questioning the adequacy of self-regulatory privacy protection measures).

\item \begin{flushright}
America Online's plan to share its customers' telephone numbers with telemarketers is an example of a privacy policy gone awry in pursuit of marketing opportunities. In mid-1997, with minimal notice to its customers, America Online amended its "Terms of Service" to provide that AOL might make the telephone numbers of AOL members available to AOL partners for telemarketing. Once the amendment was discovered, AOL received an onslaught of complaints from AOL subscribers, politicians, and privacy-rights groups, and as a result, abandoned its plans. \textit{See, e.g., Seth Scbiesel, America Online Backs Off Plan to Give Out Phone Numbers, N.Y. TIMES, July 25, 1997, at C1. \textit{See also AOL CEO Steve Case's letter to members (July 24, 1997)}<http://www.news.com/SpecialFeatures/0,5,12794,00.html>. \textit{See also PAUL M. SCHWARTZ AND JOEL R. REIDENBERG, DATA PRIVACY LAW 216-17 (1996) which states: [T]he Direct Marketing Association's (DMA) Code of Fair Information Practices stipulates that marketers should notify individuals of the collection of data for marketing purposes. The marketing departments of many companies belonging to the DMA, however, collect data directly from individuals for sale to third parties without notifying individuals. The code is not systematically honored by companies engaged in direct marketing activities.}
\end{flushright}
\end{itemize}

\begin{itemize}
\item Directive 95/46, 1995 O.J. (L281) 31. \textit{See discussion supra} Part III.B.
\end{itemize}
A. Constitutional Protections

Although a right of privacy is not specifically guaranteed by the Constitution, the U.S. Supreme Court has held that the Constitution protects a right of privacy in making certain intimate personal decisions from governmental interference. The Supreme Court has not yet held that the Constitution protects a right of privacy in personal information. However, some informational privacy protections can be found in the First and Fourth Amendments, and it seems likely the Supreme Court will hold that the Constitution protects a right of informational privacy.

1. Fourth Amendment Protections

The right to privacy from governmental intrusion is found in the Fourth Amendment's prohibition against unreasonable searches and seizures. The Fourth Amendment to the Constitution provides:

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.

Due to advancing technology and law enforcement capabilities in the Twentieth Century, the Supreme Court has been faced with a number of cases interpreting novel applications of the Fourth Amendment. When faced with its first electronic surveillance case, Olmstead v. United States, the Court ruled that no warrant was necessary for federal agents to tap a telephone wire. The majority emphasized that the Fourth Amendment was understood to protect only against "physical invasions" by law enforcement officers. In his famous dissent,

156. See Paul v. Davis, 424 U.S. 693, 713 (1976) (identifying these personal decisions as those concerning "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education").
157. U.S. CONST. amend. IV.
159. 277 U.S. 438, 466 (1928) (Brandeis, J., dissenting).
160. Id.
161. Id.
Justice Brandeis argued for an expanded notion of the nature of privacy to accommodate new technology.\textsuperscript{162} In 1967, the Supreme Court overruled \textit{Olmstead} in deciding \textit{Katz v. United States},\textsuperscript{163} and held that the interception of a telephone conversation in a public telephone booth does constitute a search and seizure for Fourth Amendment purposes.\textsuperscript{164} The court determined that the threshold question is whether there is a "reasonable expectation of privacy," as opposed to the earlier trespass requirement.\textsuperscript{165} The Court wrote:

For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.\textsuperscript{166}

In 1995, a military court addressed whether an individual has a reasonable expectation of privacy in his private e-mail.\textsuperscript{167} Citing \textit{Katz}, the court held that an individual does have a reasonable expectation of privacy under the Fourth Amendment in his e-mail communications stored and sent via an online service.\textsuperscript{168}

2. \textit{Informational Privacy and Whalen v. Roe}

The right to informational privacy was first addressed by the U.S. Supreme Court in \textit{Whalen v. Roe}.\textsuperscript{169} This case involved the invasion of patients' privacy by a New York statute requiring physicians to submit copies of prescriptions for abused drugs to the state for inclusion in a centralized computer file.\textsuperscript{170} Although the Court upheld the statute, finding that New York's interest in experimenting with solutions to control the distribution of dangerous drugs was a legitimate exercise of the state's police power, the Court re-affirmed the right of an individual to have his personal information kept private.\textsuperscript{171}

---

\textsuperscript{162}. \textit{Id.} at 471. \textit{See also supra} note 2 and accompanying text.
\textsuperscript{163}. 389 U.S. 347 (1967).
\textsuperscript{164}. \textit{Id.} at 353.
\textsuperscript{165}. \textit{Id.} at 361.
\textsuperscript{166}. \textit{Id.} at 351-52.
\textsuperscript{168}. \textit{Id.} at 576.
\textsuperscript{169}. 429 U.S. 589 (1977).
\textsuperscript{170}. \textit{Id.} at 589-91.
\textsuperscript{171}. \textit{Id.} at 596-605.
A final word about issues we have not decided. We are 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. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. 172

3. First Amendment Considerations

The First Amendment, 173 which protects speech, including commercial speech, 174 from governmental interference, also affects informational privacy. On the one hand, the First Amendment places limitations on the right to informational privacy. 175 The First Amendment free-speech and free-press goal of assuring the free flow of information is antithetical to the idea of privacy in information. Free-speech and free-press considerations imposed by New York Times Co. v. Sullivan 176 limit the applicability of the common law right of privacy torts, even those involving non-governmental actors, where the affected subject is newsworthy. 177

On the other hand, the First Amendment also provides additional information privacy protections. For instance, the First Amendment-inspired Privacy Protection Act limits governmental seizure of publishers' work product materials. 178 Because anyone posting messag-

---

172. Id. at 605. See also id. at 598-600 & nn.22-26 (noting that courts have recognized a privacy interest in avoiding disclosure of personal matters).
173. The First Amendment reads: "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." U.S. CONST. amend. I.
175. For a different perspective on conflicts between the First Amendment and property claims, see Zimmerman, supra note 33 (arguing that property claims should take a backseat to First Amendment values).
177. See discussion of common law privacy torts infra Part IV.B.
es on the Internet or online services can be considered a “publisher,” this Act may prove to have special significance.

4. State Constitutions

Some state constitutions include privacy protections which surpass privacy protections in the U.S. Constitution. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington have broader privacy protection. In California, a court has recognized that the constitutional right to privacy extends to private as well as public employers.

B. Common-Law Right to Privacy Torts

As for intrusions by non-governmental means, the common law right to privacy tort may provide some protection. The call for legal recognition of a right to privacy is generally attributed to an 1890 law review article by Louis Brandeis and Samuel D. Warren, The Right to Privacy. In this article, Warren and Brandeis advocated a right to privacy and warned that technology innovations would decrease the personal dignity of the individual if such privacy protections were not provided.

Subsequently, a common law doctrine of personal privacy has emerged as a group of four invasion of privacy torts delineated by both Dean William L. Prosser and the Restatement (Second) of Torts: (1) the unreasonable intrusion upon the seclusion of another; (2) the

---

182. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890); see also Mell, supra note 25, at 29; Richard C. Turkington, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10 N. ILL. U. L. REV. 479, 482 n.5 (1990) (indicating an 1881 Michigan case and other sources which discussed privacy a few years prior to publication of the Warren and Brandeis article).
183. Warren & Brandeis, supra note 182, at 196. Brandeis expressed the concerns he later reiterated as Supreme Court Justice in the Olmstead dissent. See 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting). See also supra note 2 and accompanying text.
186. Id. § 652B.
unreasonable publicity given to another’s private life;\textsuperscript{187} (3) the publicity that unreasonably places another in a false light before the public,\textsuperscript{188} and (4) the appropriation of another’s name or likeness.\textsuperscript{189}

1. Unreasonable Intrusion Upon the Seclusion of Another

Under this tort, “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”\textsuperscript{190} Unlike the other common law privacy torts, in which the disclosure of private information is a necessary element, disclosure is not required to establish liability for this tort.\textsuperscript{191} There is no liability if the underlying information is public record or if the activity intruded upon is conducted in a public space where one would not reasonably expect privacy.\textsuperscript{192} Because this tort has been applied to wiretaps,\textsuperscript{193} liability would likely be imposed for the unauthorized access to or interception of electronic communications and information systems.\textsuperscript{194}

2. Publicity Given to Private Life

Under this form of invasion of privacy:

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.\textsuperscript{195}

This tort seems to offer many opportunities for potential recovery in cases in which private facts are revealed electronically. Recovery under this privacy tort, however, is restricted by several judicially imposed requirements. The required publicity must be communicated to enough

\textsuperscript{187} Id. \textsuperscript{\textsection} 652D.
\textsuperscript{188} Id. \textsuperscript{\textsection} 652E.
\textsuperscript{189} Id. \textsuperscript{\textsection} 652C.
\textsuperscript{190} Id. \textsuperscript{\textsection} 652B.
\textsuperscript{192} RE\textsuperscript{STATEMENT}, supra note 185, \textsuperscript{\textsection} 652B cmt.c.
\textsuperscript{193} Id. \textsuperscript{\textsection} 652B cmt.b. See, e.g., Rhodes v. Graham, 37 S.W.2d 46 (Ky. 1931).
\textsuperscript{194} See also PERRITT, supra note 181, \textsuperscript{\textsection} 3.5.
\textsuperscript{195} RE\textsuperscript{STATEMENT}, supra note 185, \textsuperscript{\textsection} 652D.
people such that "the matter must be regarded as substantially certain to become one of public knowledge."\(^{196}\)

In addition, there will be no liability for publicity of facts that are a matter of public concern or of public record, because of First Amendment guarantees. The Restatement specifies birthdate, marital status, military record, professional or occupational licenses, and litigation as examples of public records for which there will be no liability for publication; yet, on the other hand, the Restatement specifies income tax returns as records not open to public inspection.\(^{197}\) Thus, publication of such information is actionable. In *Cox Broadcasting Corp. v. Cohn*,\(^{198}\) a case involving publication of a rape victim's identity, the U.S. Supreme Court held that under the First Amendment, publicity of matters of public record are not actionable\(^{199}\) and further that "[t]he commission of crime, prosecutions resulting from it, and judicial proceedings arising from the prosecutions, however, are without question events of legitimate concern to the public and consequently fall within the responsibility of the press to report the operations of government."\(^{200}\)

\(^{196}\) See *Tureen v. Equifax, Inc.*, 571 F.2d 411 (8th Cir. 1978) (discussing a plaintiff who sued under this tort when the consumer credit reporting firm, Equifax, submitted a life and health underwriting history report to plaintiff's health insurer (at the request of insurer) after plaintiff made health insurance benefit claims). The majority of the court held that defendant's disclosure of information to its client, the insurer, without further dissemination, was insufficient publication. *Id.* at 417.

However, Judge Heaney disagreed, stating that "[t]he collection and retention of personal information about a particular consumer by a commercial information broker such as Equifax makes the dissemination of that information sufficiently likely as to meet any reasonable requirement of 'publicity.'" *Id.* at 420 (Heaney, J., dissenting). He emphasized that "[t]he dissemination of private information by a commercial credit broker to insurance companies, banks and other customers requesting such information is no less 'public' than the posting of a debt in a creditor's shop window." *Id.* at 421 (Heaney, J., dissenting) (citing *RESTATEMENT*, supra note 185, § 652D cmt.a, ill.2, and providing an example of sufficient publicity).


*See also* *Beverly v. Reinert*, 606 N.E.2d 621 (Ill. App. Ct. 1992) (rejecting an invasion of privacy claim that was based on the unreliability of fax technology and determining that the possibility that a faxed letter might have gone to (or have been intercepted by) the wrong party was not sufficient public disclosure).

\(^{197}\) *RESTATEMENT*, supra note 185, § 652D cmt.b. The comments provide further examples of the type of information not of legitimate public interest which, if divulged, would be actionable invasion of privacy: sexual relations, "family quarrels, many unpleasant or disgraceful or humiliating illnesses, most intimate personal letters, most details of a man's life in his home, and some of his past history that he would rather forget." *Id.*

\(^{198}\) 420 U.S. 469 (1975).

\(^{199}\) 420 U.S. at 496.

\(^{200}\) 420 U.S. at 492.
This tort may be a basis for suit in cases in which personal information (i.e., medical condition, tax return, or other confidential information) is disseminated electronically to a significant number of people through a public bulletin board, newsgroup, or other means.\textsuperscript{201}

In \textit{Dennis v. Metromail Corporation},\textsuperscript{202} a pending case involving the compilation of personal data by direct marketer, Metromail, and former owner, R.R. Donnelley & Sons, suit was brought under this privacy tort. In addition, claims were filed for intentional or reckless disregard of safety, fraud, unjust enrichment, infliction of emotional distress, and negligent entrustment.\textsuperscript{203} The suit was initiated by a woman who had given her name, address, sex, age, medical condition, and buying habits to a Metromail survey in exchange for the promise of discount coupons and free products.\textsuperscript{204} The survey response was processed by a prison inmate who then sent the plaintiff an offensive, sexually graphic, and threatening letter.\textsuperscript{205} This case, which was initiated in April 1996, was later expanded to a class action including plaintiffs from California, Illinois, and New York who also responded to Metromail surveys processed by prison inmates.\textsuperscript{206} The complaint was amended to add a claim for breach of contract. In addition, the fraud claim was expanded to include Metromail's "deceptive acquisition" of information by promising to provide coupons, and then selling the information to telemarketers, bill collectors, and others, and also making the information available over a 1-900 number "people locator" service for $3 a minute.\textsuperscript{207}

The \textit{Metromail} case is particularly significant in the electronic privacy area because Metromail is one of the suppliers of the personal information that \textit{Four11}, the Internet telephone number and address directory

\begin{itemize}
\item \textsuperscript{201} See also \textit{Perritt, supra} note 181, § 3.5.
\item \textsuperscript{202} No. 9604451, (D. Texas, Travis County, filed Apr. 18, 1996).
\item \textsuperscript{203} Id.
\item \textsuperscript{204} Id.
\item \textsuperscript{205} Id.
\item \textsuperscript{206} \textit{Class Action Expands Against Metromail and Donnelley Over Privacy Violations; Broader Focus, New Plaintiffs Target Deceptive Collection and Sale of Data; Return of Profits Sought}, \textit{Bus. Wire}, Apr. 30, 1997, \textit{available in LEXIS, Nexis Library} (reporting that the case has led to federal and state legislation banning the sale of children's data without parental consent, prohibiting 900 number "look-up" services on children, and prohibiting prisoners from processing children's data).
\item \textsuperscript{207} Id.
\end{itemize}
database, LEXIS/NEXIS, and other commercial services provide in their "people-finding" databases.\(^{208}\)

3. Publicity Placing Person in False Light

Under this tort:

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.\(^{209}\)

False light invasion of privacy is similar to defamation. However, a reputation need not be injured in the same manner that is necessary for defamation liability.\(^{210}\)

This tort may provide a basis to sue for the online dissemination of erroneous information in situations in which the database provider has not taken proper steps to ensure its correctness.\(^{211}\)

4. Appropriation of Name or Likeness

Under this form of invasion of privacy, "[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."\(^{212}\) Usually this privacy invasion applies to the commercial use of another's name or likeness.\(^{213}\) Some states have extended this tort to personality as well.\(^{214}\)

This tort may be restricted by First Amendment concerns when the appropriation of a person's name or likeness for commercial use is for a newsworthy purpose. In *Stern v. Delphi Internet Services Corp.*,\(^{215}\)

---

208. See *supra* note 31 and accompanying text.
209. Restatement, *supra* note 185, § 652E.
210. Id. § 652E cmt.b.
211. See Dun & Bradstreet, Inc. v. Greenmoss Builders, 472 U.S. 749 (1985) (rejecting D&B's argument that a credit report was a matter of public interest, which would require a showing of "actual malice" under the First Amendment to be actionable for defamation, and therefore, allowing the subject of an inaccurate credit report, prepared by D&B and disseminated to five D&B subscribers, to successfully sue D&B for defamation). The Court held that the particular credit report concerned no public issue because "[i]t was speech solely in the individual interest of the speaker and its specific business audience." *Id.* at 762.
212. Restatement, *supra* note 185, § 652C.
213. Id. § 652C cmt.b.

1192
a controversial talk-show host, Howard Stern, brought suit under New York's right to privacy statutes against Delphi Internet Services Corporation after Delphi used Stern's photograph without his consent in an advertisement. Stern had announced his candidacy for governor of New York, and Delphi used Stern's photograph to advertise an online bulletin board service set up to debate Stern's candidacy. The court found that, although Delphi had used Stern's name and photograph for a commercial purpose without Stern's consent, Delphi's use was permissible because Stern's candidacy was a matter of public interest. The court analogized Delphi's service to a television network, which is both entertainer and news disseminator, stating that the incidental use by a news disseminator of an individual's name or likeness in an advertisement is protected by the First Amendment: "The newsworthy use of a private person's name or photograph does not give rise to a cause of action ... as long as the use is reasonably related to a matter of public interest."

The appropriation privacy tort may provide a basis for suit involving the sale of non-public record personal information by commercial online publishers. This tort may also provide the basis for suit against marketers of names and e-mail addresses for use by unsolicited commercial e-mailers. However, plaintiffs using this tort or similar statutes to sue the distributors of mailing lists have so far been unsuccessful.

217. Stern, 626 N.Y.S.2d at 695.
218. Id. at 698-701.
219. Id. at 698-99.
220. See Shibley v. Time Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975) (rejecting plaintiff's argument that Time Magazine appropriated his personality when it sold its subscription lists to direct mail advertisers, and holding that defendant's sale of subscription lists did not constitute "appropriation or exploitation of one's personality" as defined by Ohio common law). The Shibley court emphasized that Ohio had a statute, which survived constitutional challenges, permitting the sale of names and addresses of registrants of motor vehicles to direct mail advertisers. Id.

See also Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. 1995), appeal denied, 662 N.E.2d 423 (Ill. 1996) (alleging in a class action suit that defendants' (American Express Company and its related companies) practice of renting information regarding cardholder spending habits constituted an invasion of privacy). The Dwyer court rejected plaintiff's appropriation claim finding that "a single, random cardholder's name has little or no intrinsic value to defendants (or a merchant)" until the "[d]efendants create value by categorizing and aggregating these names [into lists of buyers by type]." Id. at 1356. The court further stated that "defendants' practices do not deprive any of the cardholders of any value their individual names may possess." Id. The plaintiffs apparently hoped
C. Other Common Law Bases for Litigation

The traditional right of privacy torts have not always been persuasive in redressing invasions of informational privacy. Those seeking judicial redress may therefore use other common law causes of action including: breach of contract; negligence; breach of confidentiality; intentional or reckless disregard of safety; fraud; infliction of

that a 1992 agreement between American Express and the New York State Attorney General, that American Express would disclose to cardholders its use of cardholder spending habits, would be influential in persuading the court. However, this agreement seemed to have no effect on the court's decision. The court, which cited Shibley frequently, also noted that Illinois has a statute, similar to Ohio's, permitting the sale of names and addresses of licensed drivers and registered motor-vehicle owners to direct mail advertisers. Id. See also Avrahami v. U.S. News & World Report, No. 95-1318 (Va. Cir. Ct., Arlington County, 1995), appeal denied, No. 961837 (Va. Sup. Ct., 1996) (raising similar privacy tort issues and also finding in favor of the defendant magazine).

221. See, e.g., discussion of Concentric Network Corp. v. Wallace, infra Part IV.E.2. Breach of contract is particularly appropriate where there is an express policy protecting user privacy. See also Peter P. Swire, Markets, Self-regulation, and Government Enforcement in the Protection of Personal Information, in NAT'L TELECOMM. & INFO. ADMIN., PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE Ch. 1 § A (1997) <http:f/www.ntia.doc.gov/reports/privacy/selftegl.htm> (arguing that a contractual approach to privacy protection should be used, in which individual privacy rights would be established through contracts made with data collection companies).

222. For instance, a negligence claim would be appropriate in a situation in which an information provider has failed to use proper techniques to safeguard the security of the data.


Attorney/client confidentiality issues arise when documents are sent or stored insecurely. See PERRITT, supra note 181, § 3.22. See also ALLISON, supra note 47, at 129-31; Oppedahl, supra note 47, at 5 (discussing risks involved in the electronic transmission of client documents and security measures).

224. See, e.g., Dennis v. Metromail Corp., No. 9604451 (D. Tex., Travis County, filed Apr. 18, 1996), discussed supra Part IV.B.2.

225. See, e.g., Dennis, discussed supra Part IV.B.2.
emotional distress; 226 right of publicity; 227 trade secret misappropriation; 228 and trespass to chattels, conversion and unjust enrichment. 229

Litigation based on common law property concepts might be most successful in redressing informational privacy violations. Property rights have been recognized in certain types of information. The U.S. Supreme Court held in Ruckelshaus v. Monsanto Co., 230 that persons have a property interest in a trade secret. Other courts have recognized an individual's property right in his medical records 231 and in his polygraph records. 232 The right of publicity, which is similar to the appropriation privacy tort in that it provides a cause of action for the use of an individual's name or likeness without his consent, is considered a property right by the courts. 233 Similarly, some courts finding invasions of privacy under either the common-law appropriation tort or state appropriation statutes, have found property rights in a person's name or likeness. 234

---

226. See, e.g., Dennis, discussed supra Part IV.B.2.

227. See, e.g., Stern v. Delphi Internet Services Corp., 626 N.Y.S.2d 694 (Sup. Ct. 1995), discussed supra note 215. The right of publicity, which is recognized by twenty-four states (and which is quite similar to the appropriation right of privacy tort), involves the right to control and profit from the commercial value of one's identity. See also J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY (1996); Elizabeth S. Perdue, Right of Publicity, in ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET 259-65 (1996).


229. See, e.g., Cyber Promotions, Inc. cases discussed infra Part IV.E.2.


233. Acme Circus Operating Co. v. Kuperstock, 711 F.2d 1538, 1541 (11th Cir. 1983). See also MCCARTHY, supra note 227, § 10.2[A].

A number of commentators favor the extension of property rights to personal information. Extending property rights protection to personal information would give individuals the rights guaranteed in the fair information practices guidelines: the right to be informed of data collection and transfer; the right to limit data collection, data transfers, and secondary uses; the right to access one's personal data and make corrections; and the right to have one's personal data maintained securely. In addition, an individual would have commercial rights in his or her personal information.

D. Statutes Providing Privacy Protections

Congress has responded to the need for informational privacy and security protections by enacting statutes in a piecemeal fashion to address specific privacy needs. The Electronic Communications Privacy Act of 1986 (ECPA) and the Computer Fraud and Abuse Act contain provisions to protect some aspects of electronic privacy. The Privacy Protection Act of 1980 restricts governmental seizure of publishers' investigative work product. The Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988 regulate government record-keeping and prevent government agencies from divulging certain personal information without proper authorization. The Fair Credit Reporting Act protects the acquisition and disclosure of information by the credit reporting industry.

235. See, e.g., ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Arthur R. Miller, Personal Privacy in the Computer Age: The Challenge of New Technology in an Information-oriented Society, 67 MICH. L. REV. 1091 (1969). See also Mell, supra note 25 (proposing a federal statute giving individuals property rights in personal information); BRANSCOMB, supra note 33, at 180 (arguing that property rights should extend to all information). But see Samuelson, supra note 230 (questioning the designation of information as property).

236. See discussion of fair information practices guidelines infra Part V.

237. See BRANSCOMB, supra note 33, at 181.


In 1986, the Electronic Communications Privacy Act (ECPA) was enacted to amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which authorized court-ordered government wiretapping. The ECPA protects against unauthorized access, interception, or disclosure of private electronic communications by the government as well as by individuals and third parties. In addition, the ECPA provides important protections for online users. The Act imposes potentially stiff penalties for violation of the statute and requires a court-ordered warrant for a governmental search of electronic communications. An electronic communication is defined by the statute as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . ." Intercept is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

Title I of the ECPA restricts the interception of oral, wire, and electronic communications while in transit, and Title II pertains to the acquisition and disclosure of stored communications. The ECPA contains numerous exceptions. Some exceptions give online service providers the power to intercept and disclose electronic communications.

---

249. Id. § 2510(4).
250. Id. §§ 2510-2521.
251. Id. §§ 2701-2710.
under certain circumstances: situations in which the service providers suspect the sender is attempting to damage the system, or when necessary for the rendition of the service (e.g. the systems operator (sysop) must review the content of the communication before forwarding it). In addition, if the communication seems to pertain to the commission of a crime, the service provider may disclose the electronic communication to a law enforcement agency.

Another exception is provided for electronic communications made to a system that is "readily accessible to the general public." The ECPA provides that interception of such communications is lawful. Therefore, the ECPA is not violated when postings to Usenet groups, listservs, bulletin board systems, and chat rooms are read and archived.

Yet another exception allows service providers and anyone else to intercept and disclose an electronic communication if either the sender or the recipient of the message consents to the inspection or disclosure. Many commercial services require a consent agreement from new members when signing up for the service. Consent may be implied in employment relationships, especially when the employer notifies employees that their e-mail will be monitored.

Finally, the ECPA provides an "ordinary course of business" exception, which may also support employer monitoring of employee e-mail. This exception is found in the definition of "electronic, mechanical, or other device" which exempts from the interception prohibition an entity which provides the electronic communication service "in the ordinary course of its business."

Cases interpreting the "ordinary course of business" provision have involved telephone monitoring, and the courts have generally held that

---

252. *Id.* § 2702(b).
253. *Id.* §§ 2511(2)(a)(i), 2702(b).
254. *Id.* § 2702(b)(6).
255. *Id.* § 2511(2)(g)(i).
256. *Id.* § 2702(b)(3).
257. *Id.* §§ 2511(2)(c).
258. *Id.* § 2510(5). The definition of "electronic, mechanical, or other device" is:

[A]ny device or apparatus which can be used to intercept a wire, oral, or electronic communication other than . . . (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

...
an employer may monitor an employee for as long as the communication is business-related.259

In *Steve Jackson Games, Inc., v. U.S. Secret Service,*260 a case involving the seizure of e-mail and stored electronic communications, the court held that U.S. Secret Service agents violated Title II of the ECPA and the Privacy Protection Act261 by seizing plaintiff’s computer equipment containing unread e-mail, software, and materials the plaintiff planned to publish, which were outside the scope of the warrant.262 The agents were searching for a confidential telephone company document that had been stolen by computer hackers and uploaded to a bulletin board operated by Blankenship, an employee of the plaintiff, Steve Jackson Games, Inc. (SJG), which also operated a bulletin board.263 The officers had no information that SJG, which operated the bulletin board system and published computer games and books, was involved in the illegal activity.264 However, the officers believed Blankenship may have uploaded the document to SJG’s bulletin board, which Blankenship used and helped operate.265 They obtained a warrant to seize a variety of files and documents from the SJG bulletin board.266

The district court found that in seizing unread e-mail and software, which were outside the scope of the search warrant, the Secret Service agents violated Title II of the ECPA’s provisions regarding stored

259. *See, e.g.,* Epps v. St. Mary’s Hosp. of Athens, Inc., 802 F.2d 412, 416-17 (11th Cir. 1986) (finding that employer monitoring of a conversation between two employees, during which one employee criticized supervisors, was in the ordinary course of business because the call took place during work hours, and it concerned supervisory employees and the work environment). *See also* Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (determining that an employer’s monitoring of a business call, in which the employee revealed trade secrets to a business competitor, was within the ordinary course of business because the employer had suspicions that trade secrets were being revealed and listened only long enough to confirm that fact). *See also* Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that the six-week monitoring of the calls of an employee suspected of wrongdoing was “well beyond the boundaries of the ordinary course of business”).

260. 816 F.Supp. 432 (W.D. Tex. 1993), aff’d, 36 F.3d 457 (5th Cir. 1994).


262. 816 F. Supp. at 439-44.

263. *Id.* at 435-36.

264. *Id.*

265. *Id.*

266. *Id.* at 435-38.
communications as well as the Privacy Protection Act. The district court rejected plaintiffs’ claim that the seizure of the unread e-mail also violated Title I of the ECPA regarding interception of communications, finding that the communications were not “intercepted” as defined by the statute because they were in storage when they were seized. The Fifth Circuit upheld this issue on appeal.

Yet in *Davis v. Gracey*, another case involving government seizure of unread e-mail and software from a bulletin board service, the court found that the police officers who seized the items did not violate the ECPA or the Fourth Amendment rights of the plaintiff, a bulletin board operator. Although the circumstances were similar to those in *Steve Jackson Games (SJG)*, they differed sufficiently to produce a different decision. Unlike the SJG bulletin board operator who had no part in the criminal activity which led to the seizure of computer items, the *Davis* bulletin board operator was selling pornographic CD-ROMS, which could also be accessed via his bulletin board service. The officers obtained a warrant to search for pornographic CD-ROMs and “equipment, order materials, papers, membership lists and other paraphernalia pertaining to the distribution or display of pornographic material. . . .” Included in the seizure were 150,000 e-mail messages and 500 megabytes of software which had been uploaded onto the bulletin board by subscribers.

The court rejected both the plaintiffs’ Fourth Amendment claims that the warrant was overbroad, and that the warrant should not have been executed in a manner resulting in the incidental seizure of e-mail and other files that were stored on the hardware and were outside the scope of the warrant. The court found the term “equipment” in the warrant supported the officers’ seizure of the computer equipment. The court also found that the seizure of the e-mail and other files was unavoidable because they were contained within the computer, and the computer was “an instrumentality of the crime.” The court further held that the officers were entitled to the ECPA’s good faith clause.

267. Id. at 439-44.
268. Id. at 442.
269. This decision was criticized by some commentators. See, e.g., Giallonardo, supra note 247. See also Cutrera, supra note 247.
270. 111 F.3d. 1472 (10th Cir. 1997).
271. Id. at 1477-84.
272. Id. at 1476.
273. Id. at 1478-79.
274. Id. at 1481.
providing a complete defense to any charges, because there was a "good faith reliance on . . . a court warrant or order."\textsuperscript{276}

Violation of the ECPA has also been among the claims utilized in litigation concerning unsolicited e-mail. Internet service providers suing a bulk commercial e-mailer, Cyber Promotions, Inc., have claimed Cyber's techniques violate the ECPA.\textsuperscript{277} These ECPA claims have not yet been addressed by the courts.

2. \textit{Computer Fraud and Abuse Act}

The Computer Fraud and Abuse Act\textsuperscript{278} (CFAA) prohibits unauthorized access of computers under certain circumstances. The following are prohibited by the CFAA:

1. knowing unauthorized computer access to national security information with the intent or reason to believe that the information will be used to injure the U.S. or to advantage a foreign nation;\textsuperscript{279}

2. intentional unauthorized access to financial information of a financial institution, credit card issuer, or consumer reporting agency;\textsuperscript{280}

3. intentional unauthorized access to a government computer, which adversely affects the government's use of the computer;\textsuperscript{281}

4. knowing unauthorized access to a federal interest computer (defined as a computer used by or for the use of government agencies or financial institutions as well as a computer which is one of two or more computers used in committing the offense, and which is accessed across the state lines\textsuperscript{282}) with intent to defraud or obtain anything of value beyond the mere use of the computer;\textsuperscript{283}

5. knowing unauthorized access to a federal interest computer with intent, or with reckless disregard of a substantial and unjustifiable risk, to damage or prevent authorized use of information in those computers

\textsuperscript{276.} Davis v. Gracey, 111 F.3d 1472, 1483 (10th Cir. 1997) (quoting 18 U.S.C. § 2702(e)).
\textsuperscript{277.} See discussion infra Part IV.E.2.
\textsuperscript{279.} Id. § 1030(a)(1).
\textsuperscript{280.} Id. § 1030(a)(2).
\textsuperscript{281.} Id. § 1030(a)(3).
\textsuperscript{282.} Id. § 1030(e)(2).
\textsuperscript{283.} Id. § 1030(a)(4).
causing loss of greater than $1,000 during a one year period, or which hinders medical treatment;\textsuperscript{284}

(6) traffic in passwords or similar information through which unauthorized access to a government computer is gained or such trafficking affects interstate or foreign commerce.\textsuperscript{285}

In a well-known case brought under the Computer Fraud and Abuse Act, \textit{United States v. Morris},\textsuperscript{286} the Second Circuit affirmed that a computer hacker, who was a graduate student in Cornell University’s Ph.D. computer science program, was guilty under the Computer Fraud Abuse Act, 18 U.S.C. § 1030(a)(5)(A) when he released a “worm”\textsuperscript{287} onto the Internet.\textsuperscript{288}

Violation of the Computer Fraud and Abuse Act has been among the claims used in litigation concerning unsolicited e-mail. Internet service providers suing a bulk commercial e-mailer, Cyber Promotions, Inc., claimed Cyber’s techniques violated the Computer Fraud and Abuse Act. In Cyber Promotion’s suit against America Online for blocking its e-mailings, Cyber also claimed that AOL’s practice violated the Computer Fraud and Abuse Act.\textsuperscript{289} The statute’s applicability in these types of cases has not yet been addressed by the courts.

The Computer Fraud and Abuse Act might also be utilized to support litigation against a direct marketer or commercial database which exceeds authorized use of personal financial information kept by a credit reporting agency.\textsuperscript{290}

\textsuperscript{284} \textit{Id.} § 1030(a)(5).
\textsuperscript{285} \textit{Id.} § 1030(a)(6).
\textsuperscript{287} A “worm” is a program that travels from one computer to another but does not attach itself to the operating system of the computer it infects. \textit{Id.} at 505 n.1.
\textsuperscript{288} Morris’s goal was to demonstrate the inadequacies of security measures on the Internet. \textit{Id.} While he instituted certain safeguards intended to prevent widespread damage, the worm replicated itself and infected machines at a much faster rate than he anticipated. \textit{Id.} at 506. As a result, many computers crashed around the country, including those at major universities, military sites, and medical research facilities. \textit{Id.} It cost an estimated $200 to more than $53,000 to deal with the worm at each installation. \textit{Id.} In finding Morris guilty, the court found that: (1) Morris exceeded the implied authorization he had to access e-mail as well as to the computers of several universities, thereby satisfying the statute’s requirement of intentional access without authorization; and (2) the government was not required to demonstrate that Morris intentionally prevented authorized use which thereby caused loss. \textit{Id.} at 506-11.
3. Privacy Protection Act

The Privacy Protection Act\(^{291}\) (PPA) ensures publishers' First Amendment rights of freedom of the press by establishing that government seizure of publishers' "work product materials" is a criminal offense unless there is probable cause to believe that the person possessing such materials is committing the offense to which the materials relate:

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.\(^{292}\)

"Work product materials [are defined as] materials, other than contraband or the fruits of a crime or things otherwise criminally possessed . . . and— (1) in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person; (2) are possessed for the purposes of communicating such materials to the public; and (3) include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material."\(^{293}\)

The PPA provides monetary damages for violations.\(^{294}\) In *Steve Jackson Games*,\(^{295}\) the court found that Secret Service agents violated the PPA and ECPA when they seized computer materials outside the scope of their warrant.\(^{296}\) The court awarded the plaintiffs $8,781 for expenses and $42,259 for damages for the PPA violations.\(^{297}\) The illegally-seized materials included work product materials protected by the PPA: drafts of a book intended for immediate publication and of magazines and magazine articles that the company was planning to publish.\(^{298}\)

\(^{292}\) Id. § 2000aa(a).
\(^{293}\) Id. § 2000aa-7(b).
\(^{294}\) Id. § 2000aa-6.
\(^{295}\) *Steve Jackson Games, Inc. v. United States Secret Serv.*, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd, 36 F.3d 457 (5th Cir. 1994). *See supra* note 260 and accompanying text.
\(^{296}\) *Id.* at 438-44.
\(^{297}\) *Id.* at 438.
\(^{298}\) *Id.* at 439-40.
As previously noted, this Act may prove to have special significance because anyone posting messages on the Internet or online services can be considered a "publisher."

4. Privacy Act

The Privacy Act of 1974\(^{299}\) is the primary statute governing the federal government’s acquisition and use of federal agency records containing personal information. The act prohibits disclosure of a record without the written consent of the subject of the record except under certain circumstances. Some of these circumstances include disclosure for a "routine use"\(^{300}\) (use compatible with the purpose for which the record was collected),\(^{301}\) for law enforcement purposes, and for protecting the health or safety of an individual.\(^{302}\) A record is defined 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. . . . \(^{303}\)

Records may contain “only such information about an individual as is relevant and necessary to accomplish” a mandated agency purpose.\(^{304}\) The statute requires that the public must be advised of the existence of databases containing personal information.\(^{305}\) Additionally, agencies must provide individuals with access to their records, as well as the opportunity to challenge their contents.\(^{306}\) The Act requires accurate accounting of disclosures and corrections of records.\(^{307}\) Records must be maintained “with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual. . . .”\(^{308}\) Agencies must also “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. . . .”\(^{309}\) The statute also applies to govern-

---

300. Id. § 552a(b)(3).
301. Id. §§ 552a(a)(7).
302. Id. §§ 552a(b).
303. Id. §§ 552a(a)(4).
304. Id. §§ 552a(e)(1).
305. Id. §§ 552a(e)(1).
306. Id. §§ 552a(d).
307. Id. §§ 552a(c).
308. Id. §§ 552a(e)(5).
309. Id. §§ 552a(e)(10).
ment contractors hired to operate agency "system[s] of records." The statute provides monetary damages and injunctive relief as civil remedies for most violations. In addition, criminal penalties are available for willful violations.

The Privacy Act was amended by the Computer Matching and Privacy Protection Act of 1988. This amendment governs agencies' computerized comparison of records for the purpose of establishing or verifying an individual's eligibility for benefits or to recoup payments on delinquent debts under benefits programs. The amendment also governs matching of personnel or payroll records among federal agencies or between federal and nonfederal entities. Excluded from the provisions of the amendment are the matching of records for: law enforcement purposes; tax collection purposes; foreign counterintelligence purposes; "routine administrative purposes" relating to federal personnel if the match is "not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;" producing aggregate statistical data without any personal identifiers; research projects for which the specific data will not be used to make decisions concerning the benefits of specific individuals.

The amendment requires certain procedures for matching programs covered by the Act. The agencies involved must prepare written agreements which specify the purpose and expected benefit of the matching program. The written agreement must describe not only the records to be matched, but also the procedures that will be used both to verify the information and to notify individuals that the information they provide in applying for benefits may be subject to matching program verification. Additionally, an agency that decides to deny benefits based on information obtained through data matching must

310. Id. § 552a(m)(1).
311. Id. § 552a(g).
312. Id. § 552a(i).
315. Id. § 552a(a)(8).
316. Id. § 552a(o).
317. Id.
verify the information, provide notice to the individual, and provide an opportunity to contest the findings.  

5. **Fair Credit Reporting Act**

The Fair Credit Reporting Act (FCRA) dictates the responsibilities of “consumer reporting agencies” in adopting reasonable procedures for supplying credit information. The Act requires these agencies to operate in a manner which is fair and equitable to the consumer, assuring the information’s confidentiality, accuracy, relevancy, and proper use. “Consumer reporting agencies” are those which regularly assemble or evaluate consumer information for the purpose of furnishing consumer reports to third parties. “Consumer report” is defined as:

any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for [credit, employment, or other purposes]...

The FCRA restricts both the circumstances under which the disclosure of consumer reports can be properly made and which parties are authorized for disclosure. The Act permits disclosure to persons who intend to use the information for credit-granting, employment, insurance underwriting, governmental license or benefit eligibility, or in connection with a business transaction involving the subject of the report. Consumer reports may also be disclosed upon court order or written request from the subject of the report. The FCRA prohibits the reporting of information more than seven to ten years old. In addition, the Act requires that the subject be advised within three days after an “investigative consumer report” is first requested. An “investigative consumer report” includes information on a consumer’s character, general reputation, personal characteristics, or mode of living, and which is obtained through personal interviews with

---

318. *Id.* § 552a(p).
320. *Id.* § 1681(b).
321. *Id.* § 1681a(f).
322. *Id.* § 1681a(d).
323. *Id.* § 1681b.
324. *Id.*
325. *Id.*
326. *Id.* § 1681c.
327. *Id.* § 1681d.

1206
neighbors and friends. The FCRA requires consumer reporting agencies to disclose to the consumer, upon request, the nature, substance, and source of the information in the file, as well as recent recipients of any consumer report on the consumer. The Act also provides procedures for dealing with the disputed accuracy of the information.

The FCRA also imposes requirements on users of consumer reports. Users of consumer reports must advise the subjects of the reports when they take adverse actions based on the report. Upon written request from the consumer, users of consumer reports must disclose any basis for adverse action other than the credit report.

The FCRA provides compensatory damages and attorneys' fees for negligent noncompliance, and punitive damages for willful noncompliance. Criminal penalties are provided for obtaining credit information under false pretenses and for the unauthorized disclosure of credit information by employees or officers of a consumer reporting agency. The FCRA gives the Federal Trade Commission (FTC) administrative powers to enforce the FCRA against violators under the Federal Trade Commission Act.

In recent years, the FTC's efforts to limit the information collected and sold by the credit bureaus have been weakened by the courts. In a 1996 case, Trans Union Corp. v. FTC, the U.S. Court of Appeals for the D.C. Circuit reviewed an FTC order that Trans Union Corporation's sale of certain "target marketing" mailing lists was a

328. Id. § 1681a(e).
329. Id. § 1681g.
330. Id. § 1681l.
331. Id. § 1681m.
332. Id.
333. Id. § 1681o.
334. Id. § 1681n.
335. Id. § 1681q.
336. Id. § 1681r.
337. Id. § 1681s.
338. 81 F.3d 228 (D.C. Cir. 1996).
339. Id. at 229. Trans Union's "target marketing" mailing lists are compiled using data from Trans Union's credit reporting database, which contains the following information: name (and aliases), addresses, social security number, phone numbers, occupation, gender, ethnic background, marital status, education, as well as credit account information. Id. See also Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995), appeal denied, 662 N.E.2d 423 (Ill. 1996) (involving an
communication of "consumer reports" for an impermissible purpose under the FCRA.\textsuperscript{340} The decision hinged on the definition of "consumer report."\textsuperscript{341} The FTC argued that the mailing lists were consumer reports because they were compiled using credit account data as well as other information in Trans Union's consumer reporting database.\textsuperscript{342} The court agreed with Trans Union's argument that its "target marketing" lists were not "consumer reports" because the "implicit information conveyed therein" was not collected "to serve as a factor in determining credit eligibility."\textsuperscript{343} The court remanded the case to the FTC, stating that "mere inclusion of a fact in a report prepared for credit eligibility purposes" does not make it a "consumer report" as defined in the FCRA.\textsuperscript{344}

It seemed that the FCRA's definition of "consumer report" might be amended in 1997. In late 1996, in response to the controversy surrounding the P-TRAK database of LEXIS/NEXIS,\textsuperscript{345} the FTC proposed that Congress amend the FCRA to "provide confidentiality protections to the following elements of consumer identification: social security number, mother's maiden name, prior addresses and date of birth" by expanding the definition of "consumer report" to include "any communication by a consumer reporting agency of any identifying information other than the consumer's name, generational designation, current address and telephone number."\textsuperscript{346} In April 1997, Senator Dianne Feinstein of California introduced the Personal Information Privacy Act of 1997,\textsuperscript{347} which would add to the definition of "consumer report": "The term [consumer report] also includes any other identifying information of the consumer, except the name, address, and telephone number of the consumer if listed in a residential telephone directory available in the locality of the consumer."\textsuperscript{348} Such an amendment would limit the amount and type of personal information that commercial online services

\begin{thebibliography}{99}
  \bibitem{340} Trans Union, 81 F.3d at 229.
  \bibitem{341} Id.
  \bibitem{342} Id. at 231-33.
  \bibitem{343} Id. at 230.
  \bibitem{344} Id. at 229.
  \bibitem{345} See supra note 31 and accompanying text.
  \bibitem{347} S. 600, 105th Cong. (1997).
  \bibitem{348} Id.
\end{thebibliography}
and information resellers could provide. However, no action was taken on the bill during 1997.

6. Other Informational Privacy Acts

Other acts protecting informational privacy include:

- Federal Records Act, which regulates the disposal of federal records ("Federal records" have been held to include the e-mail messages of government employees);
- Right to Financial Privacy Act, which prohibits access to financial records of individuals by government authorities (except for the Internal Revenue Service and agencies supervising banks);
- Family Educational Rights and Privacy Act of 1974 (FERPA), which protects student records;
- Video Privacy Act, which protects videotape rental records;
- Telephone Consumer Protection Act of 1991, which regulates telemarketing practices;
- Driver’s Privacy Protection Act of 1994, which restricts the release of motor vehicle records;
- Cable Communications Policy Act of 1984, which protects cable television subscriber information;
- Telecommunications Act of 1996, which safeguards customer information held by telecommunications carriers;
- Provisions of the Internal Revenue Code which mandate the privacy of taxpayer records.

7. State Statutes

Most states also have data protection laws which vary in their focus. Several states have laws that are similar to the federal Privacy Act and

the federal Freedom of Information Act. Other states have statutes that are similar to the ECPA or the Computer Fraud and Abuse Act, while others have laws that govern only specific sectors (such as the insurance industry).

Although existing federal and state statutes provide varying levels of informational privacy protections, all these statutes fail in some respect. For example, although the Privacy Act is relatively comprehensive, the Act governs only federal government record-keeping. As a result, there are gaps in informational privacy protection which could be rectified by the enactment of a comprehensive federal statute which would govern all record-keeping systems.

E. Fertile Ground for Litigation

1. Workplace E-mail

The issue of whether employer monitoring of employee e-mail is an invasion of privacy has generated much litigation. Courts addressing this issue have so far ruled in favor of employers who read e-mail received over the employer’s computer system. Generally these courts have held that the employees did not have reasonable expectations of privacy in their workplace e-mail.

In a 1996 decision, Smyth v. Pillsbury Co., the U.S. District Court for the Eastern District of Pennsylvania held that, under Pennsylvania law, the employee did not have a reasonable expectation of privacy in e-mail communications made voluntarily to his supervisor. Smyth involved the discharge of an at-will employee based on comments he made to his supervisor (regarding the company’s sales management, including a threat to “kill the back-stabbing bastards”) via the employer’s e-mail system. The employee’s e-mail was read by company executives even though the employer had assured its employees, including the plaintiff, that all e-mail communications would remain confidential and privileged. The court further ruled that “the company’s interest in preventing inappropriate and unprofessional

359. See PERRITT, supra note 181, § 3.15.
360. See id. § 3.20.
363. Id. at 101.
364. Id. at 98 n.1.
365. Id. at 98.
comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.\textsuperscript{366} The holdings were similar in a string of California cases.\textsuperscript{367} In \textit{Bourke v. Nissan Motor Corp.},\textsuperscript{368} the court held that the plaintiffs had no reasonable expectation of privacy in their e-mail communications because they were aware their e-mail was read by the company prior to their terminations.\textsuperscript{369} In addition, the employees had signed a statement that read: "It is company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business."\textsuperscript{370} The court rejected plaintiffs' argument that they had an expectation of privacy because they were provided system access passwords which they were told to safeguard.\textsuperscript{371} The court found that these expectations were not "objectively reasonable."\textsuperscript{372} The court further held that the California wiretapping statute\textsuperscript{373} and eavesdropping statute\textsuperscript{374} did not apply to the employer's actions of retrieving, printing, and reading plaintiffs' e-mail.\textsuperscript{375}

In another California case, \textit{Shoars v. Epson America, Inc.},\textsuperscript{376} an

\begin{itemize}
  \item[366.] \textit{Id.} at 101.
  \item[367.] Workplace e-mail was a peripheral issue in one California case, \textit{Thomasson v. Bank of Am.}, No. A061120, (Cal. Ct. App. 1994), \textit{appeal denied}, 1995 Cal. LEXIS 1843 (1995). The employee alleged that he was fired after his employer discovered, through e-mail messages that he had left in the output tray of a printer, that he also worked as a gay stripper. He claimed that the employer violated his right to informational privacy by misusing information contained in the e-mail. The court held that he had no reasonable expectation of privacy in the information that he was a stripper because a publicity photo of the employee was posted outside the theater. \textit{Id.} at 15.
  \item[368.] No. B068705 (Cal. Ct. App., July 26, 1993). In \textit{Bourke}, the plaintiff and another employee sued Nissan for wrongful termination, invasion of privacy, and violation of wiretapping and eavesdropping statutes for monitoring plaintiff's e-mail. After an e-mail system trainer randomly accessed one of plaintiff's e-mail messages which was of a personal, sexual nature, Nissan began monitoring the e-mail messages of plaintiff and others in the employee's work group, issuing written warnings to several employees. The trial court granted summary judgment in favor of the employer, and the appellate court affirmed.
  \item[369.] \textit{Id.}
  \item[370.] \textit{Id.} at 7.
  \item[371.] \textit{Id.}
  \item[372.] \textit{Id.}
  \item[373.] CAL. PENAL CODE § 631 (West 1996).
  \item[374.] \textit{Id.} § 632.
  \item[375.] \textit{Bourke, supra} note 368, at 8-9.
Epson America employee unsuccessfully sued her employer under the California wiretapping statute\textsuperscript{377} for the employer's monitoring of employee e-mail. The court ruled for Epson America, finding that provisions of the California wiretapping statutes did not extend to electronic communications.\textsuperscript{378}

A similar conclusion was reached in a case involving a government employer. In \textit{Bohach v. City of Reno},\textsuperscript{379} in which plaintiffs claimed violations of the Fourth Amendment and the federal Electronic Communications Privacy Act, the court found that the employees, whose electronic communications over the employer police department's network computer system were read by the employer police department, had no reasonable expectation of privacy in the communications.\textsuperscript{380} The employees' communications, therefore, were not protected by the Fourth Amendment.\textsuperscript{381} The court also rejected the employees' claim that the employer violated the federal Electronic Communications Privacy Act by reading their electronic communications.\textsuperscript{382} The court held that reading the employee communications did not constitute "interception" as required by the federal act.\textsuperscript{383}

However, this issue is not settled. Some state\textsuperscript{384} and federal\textsuperscript{385} laws may favor employees in some workplace e-mail situations. For example, an employee may prevail in workplace e-mail litigation by claiming that the employer's e-mail monitoring violates the Electronic

---

at Epson. Shoars had informed her co-workers that e-mail would remain confidential because she believed no one had authority to monitor e-mail. When she learned that her supervisor had been intercepting and reading all e-mail messages received or sent via MCI Mail, she demanded that he stop this practice. When she requested a private e-mail account that her supervisor would not be able to access, she was fired on the basis of insubordination. Shoars then sued the employer.

\textsuperscript{377}. CAL. PENAL CODE § 631 (West 1996).

\textsuperscript{378}. \textit{Shoars, supra} note 376, at 4. See also \textit{Flanagan v. Epson Am. Inc.}, No. BC007036 (Cal. Super. Ct, Los Angeles County, Jan. 4, 1991) (rejecting the class action certification in a related suit brought against Epson under § 631 by about 700 Epson employees whose e-mail was read).


\textsuperscript{380}. \textit{Id.} at 1233-37.

\textsuperscript{381}. \textit{Id.} at 1234-35.

\textsuperscript{382}. \textit{See discussion supra} Part IV.D.1.

\textsuperscript{383}. \textit{Bohach}, 932 F. Supp. at 1235-36.

\textsuperscript{384}. \textit{See}, e.g., \textit{Ruth Hill Bro, supra} note 179, § 26.2.3.

\textsuperscript{385}. For example, in 1997, the National Labor Relations Board (NLRB) ruled in favor of an employee who was fired for criticizing the employer's new vacation policy via the company e-mail system. In \textit{Timekeeping Systems Inc. v. Leinweber}, 323 N.L.R.B. No. 30 (Feb. 27, 1997), the NLRB ruled that employee's remarks were protected under the National Labor Relations Act as a "concerted activity," and that the employer unlawfully discharged the employee. \textit{Id.} at 6-7.
Communications Privacy Act (ECPA). However, employees claiming employer violations of the ECPA will encounter several hurdles. In the first place, employees may have difficulty convincing the courts that the employers' monitoring constitutes “interception” as required under the ECPA. Courts have so far interpreted the ECPA as requiring that monitored e-mail be in transit in order to constitute “interception,” and have refused to find “interception” where the electronic communications have been accessed while in electronic storage.

Other hurdles to be encountered by employees are two exceptions to the ECPA which generally favor employers. One exception permits the interception and disclosure of an electronic communication where either the sender or the recipient of the message consents to the interception or disclosure. Consent may be implied in employment relationships, especially when the employer has notified employees that their e-mail may be monitored. The other ECPA exception which generally favors employers is the “ordinary course of business” exception, which exempts from the interception prohibition an entity which provides the electronic communication service in the “ordinary course of its business.” So far the cases interpreting the “ordinary course of business” exception have involved telephone monitoring, and the courts have generally held that an employer may monitor an employee for as long as the communication is business-related. However, some employees have prevailed against employers who have exceeded the “boundaries of the ordinary course of business,” and it is possible that courts will rule in favor of employees in similar e-mail monitoring circumstances.


390. See, e.g., cases cited in note 259, supra.

391. For example, in Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992), the court held that the six week monitoring of the calls of an employee suspected of wrongdoing was “well beyond the boundaries of the ordinary course of business.” Id. at 1158.
2. Unsolicited Commercial E-mail

The issue of unsolicited commercial e-mail has resulted in a flurry of litigation based on privacy statutes and common law rights.\textsuperscript{392} Internet service providers, America Online, CompuServe, EarthLink, and Concentric Network Corporation, have each sued Cyber Promotions Inc., an online marketer which was sending large amounts of unsolicited e-mail to the online services' subscribers.\textsuperscript{393} Cyber Promotions also sued America Online for blocking its e-mailings.\textsuperscript{394}

In \textit{Cyber Promotions, Inc. v. America Online, Inc.},\textsuperscript{395} the U.S. District Court for the Eastern District of Pennsylvania decided that the First Amendment and the state constitutions of Virginia and Pennsylvania did not give Cyber Promotions (Cyber) the right to send unsolicited e-mail to America Online (AOL) members; and therefore, AOL had the right to block the e-mail.\textsuperscript{396} In the complaint, AOL alleged that Cyber's techniques violated the ECPA, the Computer Fraud & Abuse Act, the Virginia Computer Crimes Act, and the Virginia Consumer Protection Act.\textsuperscript{397} AOL further alleged that Cyber's techniques constituted trademark infringement and dilution, unfair competition, false designation of origin, false advertising, misappropriation, conversion, and unjust enrichment.\textsuperscript{398} In its suit, Cyber alleged that AOL's blocking of its e-mailings constituted interference with contract and unfair competition, in violation of the Computer Fraud & Abuse Act and Cyber's First Amendment free speech rights.\textsuperscript{399}

The court held that AOL was not subject to First Amendment review because "AOL is not a state actor" and none of its activities constitute state action.\textsuperscript{400} The court rejected various arguments used by Cyber to support its contention that, although AOL is a private company, AOL should be treated as a state actor.\textsuperscript{401} For instance, Cyber contended that AOL serves an exclusive public function:

\begin{itemize}
  \item \textsuperscript{392} See discussion supra Part II.B.1.b.
  \item \textsuperscript{393} In 1997, Cyber Promotions was sending out 15-20 million commercial e-mail messages a day. See Simons, supra note 58, at 55.
  \item \textsuperscript{395} Id. (consolidating America Online, Inc. v. Cyber Promotions, Inc., Civ.A. No. 96-462 (E.D. Va. 1996) with Cyber Promotions, Inc. v. America Online, Inc., No. 96-2486 (E.D. Pa. 1996)).
  \item \textsuperscript{396} Id. at 445.
  \item \textsuperscript{397} Id. at 437-38.
  \item \textsuperscript{398} Id.
  \item \textsuperscript{399} Id.
  \item \textsuperscript{400} Id. at 445.
  \item \textsuperscript{401} Id. at 442-45.
\end{itemize}
By providing Internet e-mail and acting as the sole conduit to its members’ Internet e-mail boxes, AOL has opened up that part of its network and as such, has sufficiently devoted this domain for public use. This dedication of AOL’s Internet e-mail accessway performs a public function in that it is open to the public, free of charge to any user, where public discourse, conversations and commercial transactions can and do take place.

The court responded that “[a]lthough AOL has technically opened its e-mail system to the public by connecting with the Internet, AOL has not opened its property to the public by performing any municipal power or essential public service and, therefore, does not stand in the shoes of the State.”

The court also rejected Cyber’s claims that AOL’s blocking of its e-mail violated the constitutions of Virginia and Pennsylvania. The court found no Virginia case law to support Cyber’s claim and held that Pennsylvania case law was inapplicable to the circumstances of the case.

The court also denied Cyber’s later request for a preliminary injunction against AOL’s use of its “Preferred Mail—The Guard Against Junk E-Mail” system, which allows access to Cyber’s e-mail advertisements only to subscribers who specifically request: “I want junk e-mail!” Cyber contended that AOL’s ability to advertise to its subscribers over the Internet via e-mail is an “essential facility”; and therefore, AOL “refused to deal” with Cyber in violation of the federal antitrust laws. In refusing to issue an injunction, the court held that Cyber failed to demonstrate a likelihood of success on the merits of its claim.

In *CompuServe, Inc. v. Cyber Promotions, Inc.*, the U.S. District Court for the Southern District of Ohio granted CompuServe’s request for a preliminary injunction barring Cyber from sending additional unsolicited e-mail to CompuServe subscribers. The court found that

---

402. *Id.* at 442 (quoting Cyber’s Memorandum in Support of its First Amendment Right to Send Internet E-Mail to Defendant’s Members, at 13).
403. *Id.*
404. *Id.* at 445-46.
406. *Id.* at 457-58.
407. *Id.* at 458.
409. *Id.* at 1028.
Cyber's e-mailings constituted trespass to personal property. The court emphasized that Cyber's e-mailings, which continued after CompuServe demanded the e-mailings stop, burdened the operation of the CompuServe network, and damaged CompuServe's business reputation and goodwill with its subscribers who were upset by Cyber's e-mailings.

Citing Cyber Promotions, Inc. v. American Online, Inc., the court rejected Cyber's First Amendment claims. Cyber claimed the right to First Amendment protections based on CompuServe's role as "public utility" and as "postmaster." The court rejected these analogies and held that CompuServe was not a state actor for purposes of the First Amendment.

The court also rejected Cyber's claims that CompuServe's decision to connect to the Internet was an implied invitation to the public to enter its property for business purposes. The court held that the demand by CompuServe in October 1995, that Cyber cease the e-mailings, was sufficient withdrawal of any implied invitation.

Other cases brought by Internet service providers against Cyber and its president, Sanford Wallace, have produced similar results. In Concentric Network Corp. v Wallace, the U.S. District Court for the Northern District of California granted Concentric Network (CNC) a permanent injunction prohibiting Cyber from (1) sending unsolicited e-mail to CNC subscribers; (2) sending or receiving e-mail via CNC; (3) misrepresenting that any Cyber e-mail message was sent from or condoned by CNC; and (4) distributing mailing lists containing the e-mail addresses of CNC subscribers. In EarthLink v. Cyber Promotions, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (E.D. Ohio 1997), the case was settled later, with Cyber being further enjoined from mislabelling e-mail message headers to indicate messages originated from a CompuServe account, and with Cyber agreeing to pay CompuServe $65,000 in attorneys' fees. See CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (E.D. Ohio 1997).


(CNC alleged in its complaint, No. C-96-200829 (N.D. Cal. San Jose Div. filed Oct. 2, 1996), that Cyber's techniques violated the ECPA; the Computer Fraud & Abuse Act; and constituted conversion or trespass to personal property; unjust enrichment; tortious interference with contractual relations; unfair competition under the federal Lanham Act and California Business & Professional Code; breach of contract; breach of the implied covenant; and fraud. These were dismissed without prejudice).
tions, Inc., the Los Angeles Superior Court granted EarthLink an injunction, prohibiting Cyber from sending unsolicited e-mail to EarthLink subscribers. The court determined that Cyber's actions constituted trespass to EarthLink's computer systems.

Unsolicited commercial e-mail was also the subject of the first case brought before the Virtual Magistrate Project, an experimental Internet-based arbitration service created to quickly resolve disputes occurring online. Tierney and EMail America involved an advertisement posted on America Online by a marketer, EMail America, which offered for sale five million or more e-mail addresses that could be used for bulk commercial e-mailing. The case was initiated by an America Online subscriber who petitioned for removal of the advertisement on the basis both that the advertisement was deceptive, and that bulk e-mailings, in general, are against public policy and an invasion of privacy. The Virtual Magistrate recommended that AOL remove the e-mail advertisement. However, because EMail America did not participate in the proceedings, the decision is probably not legally binding.

F. Proposed Legislation

Members of the U.S. Congress have introduced several bills in response to concerns regarding the use of personal information that is collected and published online. For example, bills introduced in the first few months of 1997 include:

- Consumer Internet Privacy Protection Act of 1997. In January, Representative Bruce Vento of Minnesota introduced this bill prohibiting

420. Id.
423. Id.
424. Id.
425. Id.
the disclosure of personally identifiable information by interactive computer services without written consent of the subscribers.

- **Fair Health Information Practices Act of 1997.** In January, Representative Gary Condit of California introduced this bill which would amend the Privacy Act and establish a code of fair information practices for health information.

- **Children’s Privacy Protection and Parental Empowerment Act of 1997.** In March, Senator Dianne Feinstein of California introduced this bill prohibiting the sale of personal information about children without parental consent.

- **Social Security On-Line Privacy Protection Act of 1996.** In April, Representatives Bob Franks of New Jersey and Wally Herger of California introduced this bill prohibiting the disclosure of Social Security numbers or other personally identifiable information by interactive computer services, without the written consent of the subject of the information.

- **Personal Information Privacy Act of 1997.** In April, Senator Dianne Feinstein of California introduced this bill prohibiting the sale and use of Social Security numbers without the written consent of the subject, and amending the Fair Credit Reporting Act to include identifying information, such as a mother’s maiden name, within the definition of confidential credit header information.

- **Federal Internet Privacy Protection Act of 1997.** In April, Representatives Tom Barrett of Wisconsin and Sue Kelly of New York introduced this bill prohibiting government disclosure of any personally identifiable educational, financial, medical, or employment record.

- **American Family Privacy Act of 1997.** In April, Representative Paul Kanjorski of Pennsylvania introduced this bill prohibiting federal officers and employees from providing access to Social Security account information or tax return information through the Internet, or without the written consent of the individual. In addition, this bill would establish a commission to study the privacy and protection afforded to government records.

---

431. See supra note 31 and accompanying text (regarding the P-TRAK matter which prompted this confidentiality concern); see also discussion supra Part IV.D.5 (regarding the Fair Credit Reporting Act).
V. PROPOSED FAIR INFORMATION PRACTICES GUIDELINES

Concerns about the proper handling of records to ensure their security and privacy have intensified with the advent of computerized record-keeping. In 1973, an advisory committee of the U.S. Department of Health, Education and Welfare (HEW) issued a report, Records, Computers and the Rights of Citizens, in which the committee recommended that a federal code of fair information practices be enacted to encompass all (public and private) computerized record-keeping systems. The proposed code included:

(1) There must be no personal data record-keeping systems maintained in secret.
(2) There must be a way for an individual to determine what information is in a record and how it is used.
(3) Individuals must have a way to prevent personal information that was obtained for one purpose from being used or made available for other purposes without their consent.
(4) Individuals must have a way to correct or amend a record of identifiable information about themselves.
(5) Organizations creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Similar principles were incorporated into guidelines adopted on an international basis in 1980, when the Organization for Economic Cooperation and Development (OECD), of which the U.S. is a member, adopted the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

---


436. Id. at xx-xxi.

The fair information practices guidelines recommended by HEW and OECD have been the foundation for guidelines issued by several U.S. committees which were created in the 1990's to address the effect of the Internet and commercial online services on the privacy and security of computerized data systems. U.S. organizations addressing these issues include the Federal Trade Commission,\(^{438}\) the Commerce Department's National Telecommunications and Information Administration,\(^{439}\) and two groups created by President Clinton: the Information Infrastructure Task Force (IITF)\(^{440}\) and the National Information Infrastructure Advisory Council (NIJAC).\(^{441}\)

The NIJAC and IITF guidelines add "education principles" to the HEW's basic tenets of fair information practices.\(^{442}\) The IITF's Education Principle suggests that personal information users (such as marketers and online services) take steps to educate the public regarding potential hazards of computer use and procedures available to minimize privacy risks.\(^{443}\) The IITF recommends that personal information users use privacy telephone hotlines, Internet privacy "help" sites, and comprehensive marketing and publicity campaigns to educate the public.\(^{444}\) As stated by the IITF:

> There are many uses of the NII [National Information Infrastructure] for which individuals cannot rely completely on governmental or other organizational controls to protect their privacy. Although individuals often rely on such legal and institutional controls to protect their privacy, many people will engage in activities outside of these controls, especially as they engage in the informal exchange of information on the NII. Thus, individuals must be aware of the hazards of providing personal information, and must make judgments about whether providing personal information is to their benefit.\(^{445}\)

The implementation of an education principle is necessary due to the novelty of cyberspace technology. Many users of online services and the


\(440\). See PRIVACY WORKING GROUP REPORT, supra note 2.


\(442\). PRIVACY WORKING GROUP REPORT, supra note 2, § II.E.25.

\(443\). Id. § II.E.25-26.

\(444\). Id. § II.E.26.

\(445\). Id. § II.E.25.
Internet need to be educated as to the manner in which communication in cyberspace is unlike traditional forms of communication. First, despite the impromptu and impermanent “feel” of cyberspace, online users need to recognize the enduring and potentially widespread nature of what they communicate electronically. For example, an ill-conceived, hastily-composed communication that is posted to a Usenet group may be captured by a search engine and be available for review by Internet users for some time. A similar communication sent via company e-mail may be stored on the network computer, to be retrieved years later in discovery proceedings. Second, online users must be reminded of the potential security breaches inherent in communications technology, including the possibility of interception by Internet service providers, network administrators, and computer hackers. Third, online users should be informed by the online services that the electronic record of their activities they leave by participating online may be utilized by the online services and third parties.

In addition, online users, as well as those who never use online services or the Internet, should be educated as to how their personal information is used by others. Massive amounts of data are maintained about individuals in government and private sector databases, creating a cyberspace persona, which is used by government, marketers, credit institutions, and others in making decisions that affect their lives.

As suggested by the IITF, education regarding the hazards of online use could take place via privacy telephone hotlines, Internet privacy “help” sites, and comprehensive marketing and publicity campaigns.

446. DejaNews, the search engine for Usenet postings, provides an excellent warning. See Deja News, Deja News Policies (visited Sept. 12, 1997) <http://www.dejanews.com/info/policy.shtml>. DejaNews’ warning, however, is only viewed by those searching DejaNews’ search engine. The warning is a mouse-click away from the main page and is not easy to find.

447. The Open Profiling Standard proposed by Netscape Communications and other Internet technology companies in May 1997, appears to be the answer to this need. See supra notes 132-35 and accompanying text. However, some commentators have questioned the efficacy of the privacy aspects of the Open Profiling Standard. See, e.g., Casey Lide, Big Cookie: What’s Behind Internet Privacy Concerns: Part II, INTERNET LEGAL PRACTICE NEWSL. (Aug. 18, 1997) <http://www.collegehill.com/lip-news/lide2.html> (highlighting the substantial direct/database marketing component of the business of VeriSign, one of the originators of the Open Profiling Standard).

448. See supra Part II.
conducted by online services, marketers, and other users of personal information which is collected online.\(^{449}\)

Additional measures are required to educate individuals regarding the collection and uses of personal information in general. Personal information users should be required to prominently post a “Privacy Warning” on any form requesting personal information. For instance, warranty cards and product sample questionnaires, which request personal information such as family income, ages of family members, hobbies, and product preferences, should contain a prominent “Privacy Warning” explaining how the requested personal information will be used. Similar warnings should be posted on Web sites which collect personal information. The “Privacy Warning” should also offer individuals an opportunity to prevent third-party use of the personal information they provide.

As a result of these efforts to educate individuals about the effect of cyberspace on their lives, individuals will be enabled to make informed decisions regarding the type of personal information they choose to reveal, thereby retaining some control over the fate of their cyberspace persona.

With the addition of an education principle, the proposed fair information practices guidelines are comprehensive, and sufficiently flexible to accommodate issues which arise due to changing technologies. These guidelines should serve as the backbone for privacy legislation. Because of new technologies, this legislation is more urgently needed today than when first proposed by the HEW in 1973.

VI. CONCLUSION

The right to informational privacy is unsettled. The United States needs a comprehensive federal policy guaranteeing individuals the right to control the collection and distribution of their personal information. Legislation which incorporates the basic tenets of fair information practices is a vital component of this policy. These tenets give individuals the right to limit data collection, data transfers, and secondary uses of the data; the right to access one's personal data and to make corrections; the right to have one's personal data maintained

\(^{449}\) See, e.g., Online Public Education Network (Project OPEN), Protecting Your Privacy When You Go Online (visited May 21, 1997) <http://www.isa.net/project-open/layout.html> (providing a thorough, well-written, online brochure prepared to educate online users as to how to protect their online privacy). Project OPEN was created by the Interactive Services Association and the National Consumers League, and is sponsored by America Online, AT&T, CompuServe, Microsoft, and NETCOM Online Communications Services. Id.
securely; and the right to be informed of data collection and transfer. This legislation would therefore place restrictions on the collection and use of personal data by the users of personal information. Personal information users would be required to explicitly inform individuals when personal information is being collected and how this information might be used. Legislation would require that personal information users give individuals an opportunity to prevent further dissemination of their personal information. Accordingly, there would be appropriate restrictions on the online publication and collection of personal information.

Further, a comprehensive federal policy would provide an enforcement mechanism which would establish sanctions against violators and offer redress for aggrieved individuals. Most effective would be legislation providing a private right of action for aggrieved individuals along with the administrative enforcement powers of a government regulatory authority.

Finally, although such a comprehensive federal privacy policy is necessary to guarantee the individual’s right to control the collection and distribution of personal information, the individual must exercise this control. Online users will still need to take responsibility for their electronic communications. They will need to be cautious about the content of these communications, and when necessary, use appropriate security measures, such as encryption, to safeguard their security. Individuals will also need to decide how much personal information to reveal when registering at Internet sites and when participating in commercial transactions. By anticipating the hazards of online use and utilizing the legal protections previously outlined, individuals will be able to take full advantage of the many educational, social, and commercial opportunities available now, and in the future, throughout cyberspace.