Pace Law Review

Volume 19
Issue 1 *Fall 1998*
Internet Law Symposium

Article 6

September 1998

Privacy in Public and Private E-Mail and On-Line Systems

Myrna L. Wigod

Privacy in Public and Private E-Mail and On-Line Systems*

Myrna L. Wigod**

Introduction

The convenience and ease of sending information via electronic mail (e-mail) has expanded its use at an exponential rate. However, the same technological strides that have made e-mail possible also represent a significant threat to privacy. Electronic eavesdropping, recording, and dissemination of private information can be accomplished with relative ease and thus legal and technical means of protection are coming to the forefront of attention. This discussion addresses the interests in, threats to, and the existing and projected protections of the privacy of e-mail communications and other information as provided by both the public Internet Service Providers (ISPs) and private employers.

I. What Is Privacy?

To evaluate protections of e-mail privacy, it is helpful to analyze the conflicting interests involved. Identification of these interests facilitates an understanding of the policy goals of various protections as well an assessment of how well those goals are being met. At its most basic level, a balance must be struck between the needs of individual privacy and autonomy, and the legitimate needs for access to potentially private information. An understanding of what privacy is may be aided by analyzing

---

* This outline was adopted from a lecture given at the 1998 Pace Law Review Symposium, *Untangling the Web: The Legal Implications of the Internet*, at Pace University School of Law on March 20, 1998.

** Myrna L. Wigod, Esq. is a partner in the Computer and High Technology group of McCarter & English, with offices in Newark, New York, Cherry Hill, Boca Raton, Wilmington, and Philadelphia. The author gratefully acknowledges the assistance of Robert Burger, an associate at McCarter & English, in the preparation of this paper.

the interests and arguments on the sides of both privacy and non-privacy.

A. *Interests In Privacy*

1. *Privacy Of Information*

Individuals have a strong need to protect their personal information. This need manifests itself in three primary areas:

Interest To Prevent Access To Personal Information - Such information includes e-mail communications as well as personal financial and medical records, which are becoming increasingly accessible on-line.

Interest To Prevent Disclosure Of Information - In some circumstances, access to information may have been permitted, but it is still important to maintain control of how that information may be disseminated.

Interest To Ensure Accuracy Of Information - If authorization to disclose information has been given, guarantees are needed to ensure the information is correct. This is especially critical regarding credit and health status.

2. *Privacy Of Autonomy*

Compromises in the security of on-line activities also raise traditional privacy concerns:

Freedom From Observation Of Personal Communications/Acts - This is analogous to traditional "Peeping Tom" issues. Regarding e-mail, this goes beyond exposure of the information communicated and includes data such as time, frequency, and duration of communications as well identification of the parties involved.

Anonymity - There may be a strong interest in remaining anonymous when making public statements or conducting financial transactions. The traditional analog here is the handing out of unsigned leaflets on political or other sensitive issues.

Freedom From Intrusion/Interference - In the on-line context, one has an interest in preventing hackers from vandalizing equipment via viruses or otherwise disrupting communications. Another problem in this area is the expanding occurrence of "junk e-mail."

B. *Interests In Non-Privacy*

Notwithstanding the strong interest in protecting the privacy rights of individuals, there are legitimate reasons why such protections should not be absolute.

1. *Law Enforcement*

To Investigate And Prevent Hackers From Gaining Access To Information - If law enforcement is to protect the privacy rights of individuals, it is necessary for such individuals to sacrifice some of their privacy. In order to investigate the potentially abusive activities of suspected hackers, law enforcement needs the legal and technical means to access private information such as e-mail messages. Thus, subject to certain limiting procedures, law enforcement may need to collect information pertaining to the hackers themselves and to the intended victims. Paradoxically, law enforcement needs access to private information in order to protect it.

To Investigate And Prevent Hackers From Disrupting Service - As e-mail and Internet access become more ingrained in serving social, educational and economic functions, law enforcement will have greater responsibility to ensure service is maintained.

To Prevent And Investigate The Use Of E-mail To Plan / Coordinate Crime - This is analogous to traditional wire-tapping of telephone lines. Individual privacy interests must be balanced against society's need to thwart criminal activity.

2. *Employment*

Observation And Documentation Of Employee Activities - Employers justify monitoring employee e-mail by claiming that surveillance is necessary to keep track of the affairs of the business. Employers argue that their e-mail systems are provided primarily for business purposes and that they should have a right to enforce this limitation. In addition, some employers use electronic surveillance to help objectively gauge productivity by logging time spent on-line or on the telephone.

Protecting The Integrity Of Employee Time Billed To Customers - In industries where employee time is directly billed to the

employer's customer, such as government contracting or the legal profession, the employer has an ethical duty to ensure that such time is billed appropriately. Therefore, employers have a need to verify that customer time is not being mischarged via abuse of company e-mail and telephone systems.

Protection Of Property And Trade Secrets - Just as law enforcement has a need to guard against theft, so do employers. Because e-mail provides an extremely easy way to disseminate sensitive company information, the ability to control such dissemination could determine the viability of an organization.

Protection Against Liability For Employee Acts - E-mail has been abused to perpetrate libel, sexual harassment, hate crimes and copyright infringement. Since employers may be held liable for the illegal acts of their employees, they must have the means to protect themselves.

3. *Marketing*

Narrowly Targeting Advertising To Interested Parties - Gaining access to personal information promotes more efficient marketing activities. This serves the dual purposes of reducing product costs by avoiding wasteful advertising and providing interested consumers with product information that might not otherwise be available.

Web Site Collection Of Visitors Information - Web sites that provide free information to the public may receive funding from advertising revenues. They may also promote marketing efficiency by providing collected demographic information to marketers.

4. *On-Line Commerce*

Parties may need to give up protection of certain types of information to promote on-line commerce. This will include disclosure of name, address, credit card, and demographic information. Examples of on-line transactions include electronic contracting, on-line purchases of information and products, and Electronic Data Interchange (EDI).

II. Who Might Violate On-Line Privacy?

A. *Government*

Different forms of law enforcement intrusion might include gaining access to the Internet Service Provider (ISP) or employer stored data, monitoring communications, tracing communications trails and habits, and accessing encrypted data.

B. *Employers*

As private e-mail service providers, employers have access to all stored employee communications data. They may also have the ability to monitor employee live communications and usage habits, subject to possible legal restrictions. A 1993 MacWorld survey showed that 22% of American businesses that responded to the survey indicated that they have searched employee files, e-mail, or other communications. For companies with more than 1000 employees, the number increased to over 30%. This monitoring is often without notice to the employees and few companies have a formal policy on the issue.

C. *Internet Service Providers (ISPs)*

ISPs can increase their revenues by collecting and disclosing profile data on their customers. They also have the technological ability to access, monitor, intercept, and disclose both live and stored e-mail communications on their systems. Such disclosure might be legally permitted either in response to law enforcement directives or to reasonably protect against liability caused by customer misuse of ISP property. America Online (AOL) recently changed its privacy policy to add subscriber phone numbers to the list of personal information that it sells to direct marketers. Previously, AOL's privacy policy prevented the disclosure of subscriber telephone numbers, while allowing the company to sell member names and addresses. The new policy took effect on July 31, 1997. While AOL will generally not disclose "navigational" or "transactional" information (such as where you go or what you buy through AOL) to third parties, it may use such information to develop member lists for companies with which AOL has a contractual marketing relationship.

D. *Site Providers*

Web site providers can closely monitor the activities of individuals that access their sites. Web sites may require a user to "sign in" in order to access the site and the site providers may aggregate and disclose such profile data (including e-mail address). In addition, site providers may store and disclose any communications made with that site, and they may trace and store a user's movements and preferences within the pages of the site.

E. *Other Users*

Other users both on public and private networks may attempt to access e-mail communications and other private information. This may be to further criminal activity or simply out of curiosity. Such invasive activity may include accessing past user discussions, searching for confidential stored information, and hacking into an ISP site.

III. Manner Of Violation

A. *Threats Against Privacy Of Information*

1. *Collecting Clickstream Data*

Because a user's connection to the Internet is made via an ISP, the ISP can monitor the user's activities and record every website visited. The observable trail of the web travel is called the user's "clickstream." In addition, web sites can also gain information regarding web movement. Based on analysis of the "packets" of data that are used to carry information within the Internet, it is possible to determine certain information from a given user's packet data (e.g. source location, e-mail address). In this way a web site can observe which pages a user visited within the current site, and can also identify the previous and next sites visited by the user. This "clickstream" data of electronic markers generated by a user's browsing activities can be aggregated, stored, and reused. Note that this aggregation of data is particularly telling if done by a site host of an Internet search engine (e.g., Yahoo). The search engine site can monitor both the type of information that a user is seeking (patterns of research), and the web sites visited to obtain that information.

2. *Cookies / Web Site Monitoring*

a. *Cookies*

A web site's server computer can track a user's activity (e.g., pages visited) within that site and collect and/or save that data in a file. Then, during the communications interchange between the server and the user's computer, the server may request that this file or "cookie" be placed on the user's hard disk. The "cookie" may then be reused to identify the user's preferences based on this historical data the next time she accesses that site. The web site may then present particular advertising targeted at the user or may route the user through particular pages on the site. In response to this practice, some newer web browsers detect when the "cookie" request is made and alert the user. If the user declines acceptance of the cookie, its transmission will be blocked. Cookies, as simple text files, do not contain executable code that could be used to transmit a computer virus or to read information residing on a user's hard disk. However, any information disclosed by a user while visiting a site (e.g. name, address, credit card number) could be stored in a cookie for later access by the web site. A cookie deposited by a particular server generally cannot be accessed or read by a different server.[1]

b. *Monitoring*

Analysis of packet data can also reveal the "Internet Provider Address" of the user's computer as assigned by the user's ISP. A request may then be sent to an Internet "name server" computer to map this IP Address to the alphabetic name assigned to a user's computer. This information may reveal the identity of the user's ISP and may be used to help ascertain a user's e-mail address.

1. A cookie may be read by another server if that second server is in the same domain as the server that originally set the cookie. For example, any server within the netscape.com domain could read a Netscape cookie, whereas a server in mydomain.com could not.

3. *Collection Of Data By Users Via On-Line Search Engines*

A number of on-line services or "search engines" are readily available to help find information on the web. While these services are essential to make productive use of the network, they may also reveal private information. In particular, some search engines are specialized to assist in gaining specific information about other users. Examples are:

WebCrawler[2] - This search engine has a "Voyeur" feature that allows others to see the result of a user's searches for information. The feature provides a sampling of the key words being used by other users so that the search results based on these keywords can be viewed. WebCrawler states that "the Search Voyeur continuously displays actual searches that people are doing on WebCrawler. [However,] WebCrawler receives over 5 million queries a day, making it impossible for anyone, WebCrawler staff included, to make the association between a particular search and the person who initiated it."[3] Given the ingenuity of the hacker community, this may not be an adequate assurance.

DejaNews[4] - This search engine catalogs and indexes more than 15,000 Usenet groups. The members of these groups are required to provide profile data prior to gaining membership to the groups, and thus these profiles are available to searching parties, as are all Usenet postings made by any given user. As an example of use of this service, the New York Times reported that a search made on privacy and cryptography advocate Tim May yielded his phone number, e-mail address, and 527 messages he had posted over the previous 18 months on various topics.[5]

Four 11[6] - This search engine is dedicated to searching its database of e-mail addresses, but many e-mail addresses

---

2. *WebCrawler* (visited Oct. 24, 1998) <http://voyeur.mckinley.com> or <http://webcrawler.com>.

3. *Webcrawler Search Voyeur* (visited Oct. 24, 1998) <http://webcrawler.com/SearchTicker.html>.

4. *Deja News* (visited Oct. 24, 1998) <http://www.dejanews.com>.

5. *See* Matthew Hawn, *As the Web Expands, So Do Serveillance Tools*, N.Y. TIMES, Jan. 6, 1997, at D5.

6. *Yahoo! People Search* (visited Oct. 24, 1998) <http://www.four11.com> or <http://people.yahoo.com>.

are not listed in the database. Currently, the database only contains the addresses of individuals that have signed up to be included in its list.

The Stalker's Home Page[7] - This web site is devoted to helping people collect information on other people via on-line resources. The site is comprised of links to other databases containing advice and information as to how to conduct personal searches.

American Information Network[8] - This for-payment service has access to additional databases. It can gain private information not available by the free services.

Altavista,[9] Yahoo,[10] Excite,[11] Lycos[12] - These popular standard search engines provide facilities to search for individuals by name. Information provided by such a search may include e-mail address, street address, and phone number.

Although most web users believe that their activities are largely anonymous, this is very likely a mistaken assumption.

4. *ISP Monitoring*

As the focal point of a user's Internet activity, the ISP stands in a unique and powerful position to access information about a person, control and monitor usage, and disclose this information to others (e.g., law enforcement, marketers). As the user's gateway to the net, it is technically possible for an ISP to monitor each mouse click and keystroke made during a session. The ISP also has complete access to any stored data or message characteristics passing through its facility, and is permitted to exploit this access within few legal limits under the Electronic Communications Privacy Act (ECPA) of 1986.[13] In addition, user profile data is usually collected upon sign-up for the service and could later be disclosed unless expressly agreed otherwise.

---

7. *The Stalker's Home Page — No More Privacy! — As Seen on the LEEZA Show* (visited Oct. 24, 1998) <http://www.glr.com/stalk.html>.

8. *AiNET* (visited Oct. 24, 1998) <http://www.ain.com>.

9. *AltaVista: Main Page* (visited Oct. 24, 1998) <http://www.altavista.digital.com>.

10. *Yahoo!* (visited Oct. 24, 1998) <http://www.yahoo.com>.

11. *Excite* (visited Oct. 24, 1998) <http://www.excite.com>.

12. *Lycos: Your Personal Internet Guide* (visited Oct. 24, 1998) <http://www.lycos.com>.

13. 18 U.S.C. §§ 2510-2522 (1994).

5. *Collection Of Data Via Voluntary Means*

Consensual Disclosure - In addition to unauthorized access to personal information, users may provide such information by "consent." Often users must fill out forms disclosing information. However, they may not fully appreciate the extent to which that information will be used. For example, Web sites and on-line vendors may request personal data before a service is provided or before an item is sold or licensed. Once released, the consumer has no further control and the released information may be placed on undesirable mailing lists.

Opt-In vs. Opt-Out Approaches - In some cases, users are provided with the option of whether they wish to disclose personal information. The manner in which this option is presented can make a difference in its effectiveness in protecting privacy. The approach favored by privacy advocates is the "Opt-in" method, where consumer information is not used unless the user affirmatively releases it. The mirror image preferred by business advocates is the "Opt-out" method, where such personal information may be freely used unless the users notify marketers otherwise. Obviously the preferred approach depends on which side of the fence one stands. In order for the option to be effective however, notice of the option must be given to users. The opt-in approach ensures that the consumer is aware of the right to choose. Under the opt-out approach, consumers may assume that the option is simply not available, or more likely will not even think about it.

Sensitive Data (e.g., Medical and Financial) - Special concerns are raised when collected information moves beyond simple identity or address data to more sensitive areas. Disclosure of medical and financial records can have a profound effect on a person's job security, ability to get insurance, ability to get credit, and numerous other critical affairs. Because medical and financial institutions in possession of private data are now on-line, there are broad concerns about the ethical responsibilities of these entities. On-line access exposes a great potential for unauthorized access and commercial disclosure of such data and thus strong legal controls are desirable. As noted however, such controls

must recognize that the need for privacy is balanced against the interests of vendors and financial institutions that have a legitimate need to evaluate creditworthiness.

On-Line Discussions - Information voluntarily provided during chat sessions and user group discussions is now available to the world via the search methods described above. Where the Internet was previously comprised of a rather small group of technically oriented individuals, such discussions are now exposed to a much broader audience.

6. *Federal Reserve Board*

In March 1997, the Federal Reserve Board (FRB) conducted a study to determine the public availability of "sensitive identifying information" about consumers, such as social security number, mother's maiden name, and date of birth. The FRB is presently seeking public comment. This initiative was triggered by the well-publicized Lexis-Nexis P-TRAK service that made this type of information readily available but that has been discontinued due to public outcry. The report's conclusions stated that, "fraud related to identity theft appears to be a growing risk for consumers and financial institutions, and the relatively easy access to personal information may expand the risk." While the FRB was asked to provide recommendations to Congress regarding legislation, the report merely stated that "[i]n considering whether any legislation is desirable, the Congress must carefully evaluate whether the availability of sensitive information poses a sufficient risk to consumers and institutions to justify new laws."

7. *Federal Trade Commission*

In 1996, the Federal Trade Commission (FTC) published a report entitled "Public Workshop of Consumer Privacy on the Global Information Infrastructure."[14] This report examined consumer privacy issues in the on-line context to promote education about the use of personal information on-line.[15] More recently, in response to a request by Congress to investigate "possible violations of consumer privacy rights by companies

14. 61 Fed. Reg. 24,499 (1996).
15. *See id.*

that operate computer data bases," the FTC published a December 1997 report titled "Individual Reference Services."[16] This report investigated the individual reference service industry, and for the most part endorsed industry guidelines that restrict access to non-public information such as social security numbers.[17] The report criticized the individual reference service industry, noting that consumers do not have access to the information collected concerning them, and have no means to correct inaccuracies.[18] Privacy advocates criticized the report for its acceptance of industry guidelines.

8. *Social Security Administration*

In March 1997, the Social Security Administration (SSA) offered its Interactive Personal Earnings and Benefits Estimate Statement (PEBES) service to provide citizens with access to their Social Security payment information. However, the service was suspended on April 9, 1997 following public concerns about the risk of improper access to personal information held by the agency.[19] The SSA now offers a modified version of the service that uses Secure Sockets Layer (SSL) technology to allow on-line requests of the PEBES, however the statement will be sent back only by paper mail. The SSA is still researching the full Interactive PEBES capability and conducted a series of national forums to hear from experts in the areas of privacy and computer security, as well as members of the public. The public forums ended on June 16 and the full report was released on September 4, 1997.[20] Privacy experts expressed support for the SSA recommendations, stating that the agency has done a good job meeting with the public, consulting with experts and developing sensible standards to protect personal information. The SSA experience with Internet service delivery is being watched closely by other federal agencies as well as private companies

16. Robert Pitofsky et al., *Individual Reference Services* (visited Oct. 24, 1998) <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm#IndividualReferenceServices>.

17. *See id.*

18. *See id.*

19. *See* Notice of Social Security Forums: Privacy and Customer Service in the Electronic Age, 62 Fed. Reg. 23,525, 23,526 (1997).

20. SOCIAL SECURITY ADMINISTRATION, PUB. NO. 03-012, PRIVACY AND CUSTOMER SERVICE IN THE ELECTRONIC AGE: REPORT TO OUR CUSTOMERS (1997).

which hope to take advantage of the Internet and avoid public concerns about privacy.

9. *Compromise Of Medical Records*

While leveraging modern advances in information technology, the health care industry's placement of patient medical records in computer databases has created a potential for abuse of individual privacy. The ease of electronic networking and sharing of information has caused concern that sensitive data will be accessed and misused. Negative results of the proliferation of private data may include loss of job, denial of insurance and commercial exploitation or "data mining." Presently, there is no federal statute for blanket protection of the confidentiality of medical records, but there is an initiative in the works to pass such a law. In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to regulate the health insurance industry "to combat waste, fraud, and abuse."[21] The law contains particular provisions to assure that medical information is utilized in a manner that appropriately protects the confidentiality of the information and the privacy of individuals receiving health care services and items.[22] HIPAA established standards for confidential transmission of electronic records, levied criminal sanctions for wrongful disclosure of individual's identifiable health information, and required the Secretary of Health and Human Services (HHS) to recommend to Congress standards for protection of privacy of individually identifiable records.[23] The purpose of these recommendations was to 1) permit patients to copy records and propose corrections, 2) require health care organizations to explain how records will be disclosed, 3) allow patients to control access to information, 4) permit patients to control the use and disclosure of information, and 5) make unauthorized disclosure a crime.

Notwithstanding the aforementioned recommendations, Congress determined a number of situations in which health

21. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.).

22. *See id.* §§ 264, 1177, 2713, 110 Stat. at 1966, 2033, 2029.

23. *See id.* §§ 264(a), 306(k)(5)(A)(viii)(B)-(C), 1177, 110 Stat. at 2029, 2032, 2033.

care information will be disclosed without the patient's consent. These disclosures may be:

for health care and payment (however the patient may restrict disclosures of certain information or to certain persons);
for health oversight to licensed providers, government agencies, and medical organizations;
to protect the public health;
for research, subject to government authorization;
in emergency situations;
to next of kin;
to law enforcement; or
in judicial proceedings.[24]

B. *Threats To Communications*

1. *Access To Private Communications*

One's on-line communications do not enjoy the level of privacy that is generally afforded other communications means, such as public telephone and traditional mail. As noted, private e-mail messages may be monitored, stored and disclosed by ISPs and employers, subject to certain limitations. In addition, e-mail messages to web sites, vendors or any other party may be stored and later disclosed. In contrast to telephone communications that are rarely recorded for later use, e-mail messages are always recorded unless the recipient affirmatively destroys them. Computer technology provides a simple means to reproduce, edit, or disclose such messages.

2. *Anonymity*

Again, in contrast to some traditional venues, on-line technology makes it difficult for an individual to speak anonymously. Controversial speech or ideas may not be able to be disseminated without the speaker's identity being clearly known. Thus, this infringement on privacy spills over into the area of the First Amendment.[25] It is also difficult to purchase items on-line without leaving an audit trail identifying who the purchaser was. This may be contrasted with familiar cash

24. *See* 42 U.S.C. § 1320d-61 (1996).
25. U.S. CONST. amend. I.

transactions in which the trail of hands through which money has passed is unknown.

3. *Intrusion*

Junk E-mail Or "Spamming"[26] - While "cookies" and other unauthorized access to one's computer are obvious forms of intrusion, junk e-mail "bombings" or "spamming" may be a primary threat to the overall usefulness of the e-mail system. In addition to clogging or slowing down the entire system, mass mailings of unwanted messages could distract users from important messages and ultimately make an individual's e-mail account impractical to use. Junk e-mail may also increase a user's per minute on-line or telephone charges. While junk e-mail is a potential threat, recent cases have curtailed its use:

CompuServe, Inc. v. Cyber Promotions, Inc.[27] - In this case, mass advertising e-mailer Cyber Promotions sent thousands of unsolicited e-mail advertisements to CompuServe customers.[28] In addition, Cyber configured its computers so that the messages falsely appeared to originate from a CompuServe address.[29] This caused large numbers of undeliverable messages to be "returned" to CompuServe for storage.[30] The court granted an injunction to CompuServe based on unfair competition and conversion claims,[31] holding that the excessive storage required for the undeliverable messages consumed the capacity of several of CompuServe's computers, thereby representing an actionable trespass to chattels for which the First Amendment provided no defense.[32]

Cyber Promotions Inc. v. America Online Inc.[33] - In this case, Cyber used the same tactics against AOL as it did against CompuServe, but AOL retaliated by blocking the incoming messages from Cyber.[34] In two separate proceedings, a Pennsylvania court found that (1) AOL's blocking of messages could not deny Cyber's First Amendment rights because AOL was not a state actor, and

---

26. Lately, the term "spamming" has been used to refer to any unsolicited junk e-mail or posting scheme, while previously, the term "spam" only referred to mass postings on Usenet listings.

27. 962 F. Supp. 1015 (S.D.Ohio 1997).

28. *See id.* at 1017.

29. *See id.* at 1019.

30. *See id.* at 1022.

31. *See id.* at 1028.

32. *See CompServe*, 962 F. Supp. at 1022.

33. 948 F. Supp. 456 (E.D.Pa. 1996).

34. *See id.* at 460.

(2) AOL had not violated anti-trust laws because its e-mail service was not an "essential facility" under anti-trust law.[35]

Cyber Promotions, Inc. v. Apex Global Information Services, Inc.[36] - After the above disputes, ISPs refused to provide service to Cyber as a customer.[37] One such ISP, Apex Global Information Services, Inc., cut off Cyber's existing service without notice.[38] Cyber sued Apex under breach of contract and succeeded in obtaining a preliminary injunction from the court, ordering Apex to restore service for a six-week period while Cyber made other arrangements for Internet access.[39] As a result, Cyber is now setting itself up as a specialized ISP to send unsolicited mass mailings for its advertising customers. However, several states are considering legislation that would make the sending of unsolicited ads directly to e-mail accounts a misdemeanor.

Usenet Spamming - Another type of on-line advertising spamming abuse occurs when an advertiser posts a commercial message to a large number of Usenet news groups or to the members of an e-mail mailing list. In one case, when a pair of lawyers engaged in spamming to advertise their "Green Card" services for immigrants, the outraged Usenet readers retaliated by publishing protest messages, implementing software to erase future messages by the lawyers, and placing fake pizza orders to the lawyers' address. While there was never a legal action involved, the on-line social pressure forced the lawyers to cease their activity.

IV. Legal Protections And Limits

A. *Federal Constitution*

Any privacy protections afforded by the federal Constitution are limited by the state action requirement. Constraints on access to private information and communications arising from the Constitution apply only to Government entities and not to private parties like ISPs or employers. There are three potential sources of protection:

35. *See id.* at 457-58.

36. 1997 WL 634384 (E.D.Pa. Sept. 30, 1997)(No. CIV. A. 97-5931).

37. *See id.* at *1.

38. *See id.*

39. *See id.*

1. *First Amendment*[40]

First Amendment protections limit the government's ability to seize data where such intrusiveness would interfere with the ability to publish or distribute speech. The Privacy Protection Act (PPA), as discussed below, was enacted in 1980 to protect publishers' First Amendment right to freedom of the press against government interference.[41]

Steve Jackson Games, Inc. v. U.S. Secret Service[42] - The Secret Service, in pursuit of a hacker group, seized computers and other materials of a company's electronic bulletin board system (BBS).[43] The court held that the PPA protects persons "reasonably believed to have a purpose to disseminate to the public a newspaper, broadcast, or other similar form of public communication. . ." and awarded damages for lost business caused by the seizure of First Amendment materials.[44]

2. *Fourth Amendment*[45]

The primary source of protection in the on-line context stems from the Fourth Amendment prohibition against unreasonable searches and seizures. As a threshold matter, the Fourth Amendment can only afford protection to e-mail communications if the affected party has a reasonable expectation of privacy in such communications.

United States v. Maxwell[46] - In this case, where e-mail was being used to transmit child pornography, the court found a reasonable expectation of privacy, stating that the "appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers."[47] The ECPA, discussed in detail below, provides further law in the on-line search and seizure area.

---

40. U.S. CONST. amend. I.
41. *See* 42 U.S.C. § 2000aa (1996).
42. 816 F. Supp. 432 (W.D. Texas 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).
43. *See id.* at 437.
44. *Id.* at 440; *See* 42 U.S.C. § 2000aa(a) (1996).
45. U.S. CONST. amend. IV.
46. 42 M.J. 568 (A.F.C.C.A. 1995).
47. *Id.* at 576.

United States v. Charbonneau[48] - Conversely, a reasonable expectation of privacy was not found in statements made on-line in a private Internet "chat room."[49] In this case, an FBI operative entered chat rooms posing as a pedophile and monitored conversations regarding the transmission of child pornography.[50] When the defendant claimed that his statements made in the chat room were protected by the Fourth Amendment, the court stated that

> [d]efendant could not have a reasonable expectation of privacy in the chat rooms. Accordingly, the e-mail sent by Defendant to others in a "chat room" is not afforded any semblance of privacy; the government may present the evidence at trial. In addition, all e-mail sent or forwarded to the undercover agents is not protected by the Fourth Amendment.[51]

Thus, the expectation of privacy found in *Maxwell* did not extend to e-mail messages after they had been received by the intended recipient.[52]

3. *Second Amendment*[53]

While the government has placed restrictions on the export of encryption software, it can be argued that this is a violation of the right to bear arms. Since encryption software has been classified as "munitions," it is arguable that this places such software under Second Amendment protection.[54] There is no case law on this issue to date.

B. *State Constitutions*

While state constitutions typically provide provisions similar to those of the federal Constitution, states are free to add additional protections above the "floor" of the federal Constitution. These additional protections may also extend to private actors.

---

48. 979 F. Supp. 1177 (S.D. Ohio 1997).
49. *See id.* at 1185.
50. *See id.* at 1179.
51. *Id.* at 1185.
52. *See id.*
53. U.S. CONST. amend. II.
54. *See* 22 C.F.R. § 121.1 (1998).

C. *Federal Statutes*

1. *ECPA (Anti-Wiretapping Statute)*[55]

a. *Basic Provisions Of The ECPA*[56]

The Electronic Communications Privacy Act of 1986, which amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, is the only federal statute that specifically addresses interception and access of electronic communications. The ECPA prohibits the unauthorized interception, access, disclosure, and use of the contents of electronic and wire communications subject to certain exceptions discussed below.[57] These provisions apply to both government and private actors, and violation may result in criminal, civil, and attorney fee liability.[58] Evidence seized by the government in violation of the ECPA is subject to the exclusionary rule.[59] Because the ECPA extends only to the contents of communications, transactional information associated with electronic communications, such as the existence of the communications, identities of parties, message length, duration of communications, and e-mail title headers, are not protected.[60] The ECPA also distinguishes between live communications and stored communications as further discussed below.[61]

b. *Title I - Access To Live Communications*

Title I of the ECPA regulates interception of oral, wire, and electronic communication by government, ISPs, and employers (as well as other third parties).[62] In the absence of consent, interception of content is restricted except as a necessary incident to:

rendering the communications service,
protecting the service provider's rights/property, or

55. 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
56. *See* 18 U.S.C. § 2510 (1994).
57. *See* 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
58. *See* 18 U.S.C. § 2701 (1994).
59. *See* 18 U.S.C. § 2515 (1995).
60. *See* 18 U.S.C. §§ 2520, 2521, 2707 (1986).
61. *See* 18 U.S.C. § 2511(2)(a)(i)(h) (1994).
62. *See id.* §§ 2510, 2701.

conducting a normal course of business (as discussed further below).[63]

Thus random monitoring or managing of message streams is not restricted because it furthers the rendering of service. Interception is also permitted under reasonable suspicion of violation of ISP's rights or property.[64] ISPs and employers have much more latitude than the government, since the government may only intercept communications with a warrant upon probable cause. Note, however, that all interception is permitted with consent of one of the parties to a communication.[65]

c. *The Ordinary Course Of Business Exception*[66]

Intercept under the ECPA 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."[67] In turn, electronic, mechanical, or other device is defined to mean any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than 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.[68] Because the statute focuses on telephone or telegraph devices, it is not clear if these definitions are applicable to e-mail. To date, this exception has only been applied to telephone monitoring, but the results may also apply to e-mail privacy disputes. The major cases interpreting this provision are not entirely consistent in their interpretation of whether devices are

63. *See* 18 U.S.C. § 2511(2)(a)(1) (1995).
64. *See id.* § 2511.
65. *See id.* §§ 2511(c)-(d).
66. *See* 18 U.S.C. § 2511(2)(a)(1) (1995).
67. 18 U.S.C. § 2510(4) (1986).
68. *See id.* § 2510.

used in the ordinary course of business. These cases are summarized as follows:

James v. Newspaper Agency Corp.[69] - In this Tenth Circuit case, an employer was held exempt from ECPA liability under the ordinary course of business exception where employees were provided with advance notice of monitoring, monitoring equipment was openly installed, and no employee protested at the time of installation.[70] The employer successfully argued that equipment used to monitor customer phone calls was necessary to address concern over abusive language used by customers regarding their bills and to assist in the training of employees.[71]

Briggs v. American Air Filter Co.[72] - In this case, a supervisor monitored a business call in which an employee divulged trade secrets to a competitor.[73] The employee's supervisor had particular suspicions about confidential information being disclosed to a business competitor, had warned employee not to disclose such information, and knew that a particular telephone call was with an agent of the competitor.[74] The court found that it was within the ordinary course of business for the supervisor to listen in on an extension phone for at least as long as the call involved the type of information he feared was being disclosed.[75] The court further noted that employer monitoring that is limited to specific occasions is less intrusive than a general practice of surreptitious monitoring.[76]

Watkins v. L.M. Berry & Co.[77] On facts similar to those of *James*,[78] the Eleventh Circuit was presented with an issue that was never reached in *Briggs*; whether the contents of a personal call can ever be monitored in the ordinary course of business.[79] In response to this issue, the court held that employer monitoring of personal calls of a telemarketing employee beyond the ex-

---

69. 591 F.2d 579 (10th Cir. 1979).
70. *See id.* at 582.
71. *See id.* at 581.
72. 630 F.2d 414 (5th Cir. 1980).
73. *See id.* at 416.
74. *See id.* at 416, 420.
75. *See id.* at 420.
76. *See id.* at 420 n.9.
77. 704 F.2d 577 (11th Cir. 1983).
78. *See id.* at 583 (citing James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979)).
79. *See Watkins*, 704 F.2d at 583 (citing *Briggs*, 630 F.2d 414).

tent necessary to determine that the calls are personal in nature was not within the ordinary course of business.[80]

Deal v. Spears[81] - In this case, a store owner suspected an employee of theft and attached a device to record all her telephone conversations over six weeks.[82] Notwithstanding the legitimate purpose of the monitoring, the court followed *Watkins* and held that the privacy intrusion was "well beyond the boundaries of the ordinary course of business."[83] The employer argued that, as in *Briggs*, a telephone extension was used to monitor an employee suspected of harmful activity.[84] However, the court noted that the use of a recording device to continuously monitor over an extended period of time went beyond the permissible standards of *Briggs*.[85] As noted, the statutory definitions and court cases are specifically oriented to telephone conversation monitoring. The extent to which the business use exception will be extended to employee or Internet e-mail is unknown at this time.

d. *Title II*[86] - Access To Stored Communications

Title II regulates access to communications that are "stored" within ISP or employer facilities.[87] The basic rule for stored communications is that there are virtually no protections or restrictions on ISPs or employers regarding access. A problem here is that this provision essentially overshadows any protections available under Title I. When considering e-mail and other on-line communications, virtually all on-line communications may be technically classified as "stored" at one point or the other. Even during an interactive "chat" session, the communications are generally placed in storage while the session is occurring. One recent case has provided some guidance with regard to the distinction between interception of live communications under Title I, and access to stored communications

80. *See id.*
81. 980 F.2d 1153 (8th Cir. 1992).
82. *See id.* at 1155.
83. *Id.* at 1158.
84. *See id.* at 1157, 1158.
85. *See id.* at 1158 (citing Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. 1980)).
86. 18 U.S.C. § 2701 (1996).
87. *See id.*

under Title II. In *United States v. Moriarty*,[88] the court held that an individual that listened to stored voice mail messages could only be prosecuted under Title II and not Title I.[89] The fact that the defendant had "listened to the human voice" was not sufficient to implicate the interception provisions of Title I, and the court held that charges under both Title I and II were multiplicitous in violation of the double jeopardy clause.[90]

e. *Disclosure Under The ECPA*

In addition to access, both Title I and II regulate the disclosure of wire and electronic communications by ISPs and employers. Under the statute, such accessed communications may be disclosed:

to an intended recipient;
to anyone with consent of the originator or recipient (which could possibly be the ISP or employer itself);
to anyone, if such disclosure is necessary to continue providing service or to protect the ISP (such disclosure could be to another ISP if related to providing service);
to law enforcement pursuant to wiretap order, warrant, or subpoena; or
to law enforcement if a criminally suspicious communication was inadvertently obtained (e.g., via random monitoring).[91]

2. *Privacy Protection Act of 1980*[92]

a. *Basic Provisions Of The PPA (Privacy Protection Act Of 1980)*[93]

The PPA was enacted for the purpose of protecting the right of freedom of the press under the First Amendment, allowing publishers to investigate and develop sensitive news stories without fear of government interference. The PPA establishes safeguards protecting "publishers" from government search and seizure of materials in their possession in the ab-

88. 962 F. Supp. 217 (D. Mass. 1997).
89. *See id.* at 220.
90. *See id.* at 222.
91. *See* 18 U.S.C. § 2510 (1996).
92. 42 U.S.C. § 2000aa (1996).
93. *Id.*

sence of probable cause.[94] Probable cause in this context requires a stricter standard than under Fourth Amendment jurisprudence. Under the PPA, a warrant will only issue if there is probable cause to believe that information materials themselves are involved in the commission of a crime.[95] The PPA protects both "work product" (meaning materials prepared by the publisher or author), and "documentary materials" (meaning supporting records, photographs, interviews, and the like).[96]

b. *Application To On-Line Systems*

On-line systems and users are protected by the PPA if they provide publishing services (e.g., electronic newsletters) or engage in publishing related activities (e.g., collection of documentary information via e-mail).[97] Protection extends to the entire on-line system on which publishing materials are kept.[98]

c. *Remedies And Defenses*

Violation of the PPA may be sanctioned by an award of monetary damages, but illegal evidence so seized is not subject to the exclusionary rule.[99] Law enforcement may defend a violation of the PPA by claiming a "good faith belief" in the propriety of the seizure.[100] In *Steve Jackson Games*, at least with regard to the initial actions by the Secret Service, the court accepted the defense that the agents did not know that the PPA applied to ISPs.[101] Note that in *Steve Jackson Games*, the plaintiffs successfully sued under both the PPA and ECPA.[102]

3. *Telephone Consumer Protection Act Of 1991*[103]

The Telephone Consumer Protection Act (TCPA) of 1991 was enacted to address consumer concerns regarding privacy

94. *See id.* §§ 2000aa(b)(1), 2000aa(a)(1).
95. *See id.* §§ 2000aa(b)(1), 2000aa(a)(1).
96. *See id.* § 2000aa(a).
97. *See id.* § 2000aa(b).
98. *See* 42 U.S.C. §2000aa-7(a) (1996).
99. *See id.* §2000aa-6(e).
100. *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Texas 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).
101. *See id.* at 436.
102. *See id.* at 439.
103. 42 U.S.C. § 227 (1991).

intrusions from the telemarketing industry.[104] Under this statute, the FCC may direct a company to maintain "do not call" lists to prevent customers on such from being contacted.[105] The TCPA also makes it unlawful to solicit with an automated dialing system where the consumer is charged for the call.[106] This provision has a potential application to intrusion via junk e-mail since consumers typically pay for connect time during receipt of such messages. This issue was raised by a CompuServe customer in a suit filed regarding a CompuServe/VISA advertisement received by e-mail; however, the dispute was settled out of court.

4. *Federal Records Act*[107]

The Federal Records Act was passed in 1950 to establish the National Archives and Records Administration for the purpose of creation, maintenance, management, and disposal of the official records of federal agencies.[108] This act prohibits the disposal of records by agencies without the approval of the Archivist.[109] It is important with respect to privacy because government e-mail messages have been held to be official federal records subject to the act. In *Armstrong v. Executive Office of the President, Office of Administration*,[110] the court held that computer back-up tapes containing e-mail messages from the Reagan / Bush era were official records that could not be erased.[111] Thus, government employees should be aware that any personal information that they include in office e-mail messages are archived and may be available for public scrutiny.

5. *Communications Assistance For Law Enforcement Act (CALEA) (Digital Telephony Law)*[112]

Traditionally, law enforcement has been able to "tap" analog telephone lines under a proper wiretap order for the purpose

104. *See id.*
105. *See id.* § 227(c)(1)(A).
106. *See id.* § 227(b)(1)(A).
107. 64 Stat. 583 (1950).
108. *See id.*
109. *See* 44 U.S.C. § 2108(a) (1984).
110. 1 F.3d 1274 (D.C. Cir. 1993).
111. *See id.* at 1281.
112. 47 U.S.C. § 1001 (1994).

of investigating crime. However, the nation's telephone lines are rapidly shifting from analog to digital technology and, with this shift, comes an increased technical difficulty in the ability to eavesdrop on conversations. In the analog world, simple access to the wires through which a telephone conversation flows provides the opportunity to "listen in" on the conversation. However, when voice communications are digitized, they are sent as discrete packets of data that are multiplexed in with other data and possibly routed through different paths before being reassembled at the destination site. Thus, from a technical perspective, it becomes much more difficult to perform surveillance of communications made via digital telephony. In response to this development, the FBI successfully lobbied Congress to pass a new law to facilitate "wire tapping" of digital communications in order to restore the status quo. The 1994 CALEA (Digital Telephony Law) requires the telephone industry to conform its networks to allow for wiretapping via advanced switching equipment.[113] At the same time, the law requires that government pay for any advanced features that are not readily available.[114] The FBI is presently developing rules and proposals on how to implement the law.

As related to e-mail, the law has significant provisions whereby it:

> requires a court order for law enforcement to obtain e-mail addresses and other similar transactional data from ISPs;[115]
> specifically excuses ISPs from modifying their equipment to facilitate authorized government interception (however, ISPs are still subject to ECPA disclosure requirements regarding messages);[116]
> does not limit rights to use encryption.[117]

This last point is important because, even if law enforcement has the capability to tap digital phone lines, it would be frustrated if messages passing through these lines are protected by strong encryption. This means that law enforcement will continue to support measures such as Clipper that provide government with the technical means to de-encrypt private

113. *See id.* § 1002(a).
114. *See id.* § 1007(c).
115. *See id.* § 1002(a).
116. *See id.* § 1002(b)(2).
117. *See* 47 U.S.C. § 1002(b)(3).

messages. Since the enactment of CALEA, there have been continued delays in its implementation due to disputes between the FBI and industry. The discussions broke down after industry negotiators concluded that the FBI was seeking to significantly broaden its surveillance powers and require many more technical changes than CALEA envisions. However, following a meeting with Attorney General Janet Reno and FBI Director Louis Freeh on March 6, industry executives agreed to resume negotiations over implementation of the act. The impasse has delayed implementation of CALEA, which required new wiretap-friendly technology to be in place by October 28, 1998.[118]

6. *Privacy Act Of 1974*[119]

a. *Background*

The Privacy Act of 1974 was an amendment to the Freedom of Information Act (FOIA),[120] aimed at increasing the privacy protections of the FOIA. While the FOIA's primary goal is to make government information available to the public, it also contains exceptions that restrict disclosure of certain information in an effort to protect privacy.[121] The Privacy Act was created to further prevent government from disclosing computer database records maintained on an individual for any other purpose than that originally intended without consent. The act was amended by the Computer Matching and Privacy Act of 1988,[122] which limits government use of database "matching" techniques to aggregate information on individuals and then terminate benefits without notice and a hearing.[123]

b. *Basic Provisions*

As previously stated, the Privacy Act regulates government disclosure of information within its databases. The existence of databases of personal information must be made known to the public.[124] The Privacy Act does allow information in these

118. *See id.* § 1001 (notes).
119. 5 U.S.C. § 552a (1974).
120. 5 U.S.C. § 552 (1996).
121. *See id.* § 552(b)(6).
122. Pub.L.No. 100-503 (1994).
123. *See* 5 U.S.C.A. § 552(a) (notes) (West 1994).
124. *See* 5 U.S.C. § 552(a) (amended 1996).

databases to be disclosed to law enforcement, credit reporting agencies, and to protect the health and safety of the individual.[125] However, when information is requested on an individual, that person must be informed of the purpose of the disclosure and the uses to which the information will be put.[126] The individual may request review and amendment of such records, and disclosure must only be with written consent, unless disclosure is for a "routine use."[127] This "routine use" exception tends to negate much of the Act's privacy protection by allowing an agency to disclose a record concerning an individual, if such disclosure is for a purpose that is specifically compatible with the purpose for which the information was gathered.[128] Violations of the Privacy Act may be redressed by money damages and injunctive relief.[129] However, the Privacy Act is only effective against government disclosure of private facts; it has no effect on private entities.[130]

c. *Critics Of The Privacy Act*

Privacy advocates have criticized the effectiveness of the Privacy Act and have called for stronger protections especially in light of expanding computer networking. The American Civil Liberties Union (ACLU) has charged that the Privacy Act only mildly deters government exploitation of private information. They argue that social security numbers are being increasingly misused and as an example point to the mandatory reporting of children's Social Security Numbers (SSN) on tax forms. The act is also criticized because of its specific exception that allows government disclosure without consent if the disclosure is a "routine use" of the information.

125. *See id.* § 552(b)(7).
126. *See* 5 U.S.C. § 552 Executive Order 12600 §1 (1987).
127. *See* 5 U.S.C. § 552 Executive Order 12291 (1981).
128. *See* 5 U.S.C.A. § 552(a) (notes) (West 1994).
129. *See* 5 U.S.C.A. § 552(a) (note 6) (West 1994).
130. *See* 5 U.S.C. §552(a) (1996).

7. *Acts Protecting Financial Information*

a. *Fair Credit Reporting Act (FCRA)*[131]

Although the FCRA does not provide protections against privacy incursions by non-government actors, other statutes do provide protection in the area of financial information. The FCRA regulates disclosure of personal information by credit reporting agencies, but not the collection of this information.[132] Under the FCRA, credit bureaus must maintain procedures to protect against reporting inaccurate or obsolete credit information, and allow consumers to review their records and correct inaccuracies.[133] Credit reports may only be disclosed with permission, under court order, or for certain enumerated purposes (e.g., credit, insurance, employment, government benefits eligibility, and legitimate business needs).[134] A major weakness of the act from a privacy perspective is that agencies are not required to notify individuals of the existence, content, or use of financial records. Thus, enforcement of the FCRA may actually provide little privacy protection.

b. *Right To Financial Privacy Act (RFPA) Of 1978*[135]

This act was passed to overturn *United States v. Miller*,[136] which held that an individual had no reasonable expectation of privacy in records held by a bank.[137] The RFPA response was to set procedural restrictions on federal agency access to a bank's records of its customers. However, the financial institution may notify law enforcement if it has a suspicion of crime. Disclosure may then be authorized by warrant, subpoena, or consent. The act has no applicability to disclosure to non-government entities.

c. *Related Statutes*

Other related acts that regulate disclosure and consumer reporting of financial information are the Fair Credit Billing

131. 15 U.S.C. §§ 1681–1681(t) (1994).
132. *See id.* § 1681(b).
133. *See id.*
134. *See id.*
135. 12 U.S.C. § 3401 (1994).
136. 425 U.S. 435 (1976).
137. *See id.* at 442.

Act of 1974;[138] Fair Debt Collection Practices Act of 1977;[139] Equal Credit Opportunity Act of 1974;[140] and the Electronic Fund Transfer Act of 1978.[141]

8. *Acts Protecting Medical Records*

At the present time, there is no federal statute that protects the confidentiality of medical records. However, there is an initiative in the works to pass such a law. Some states have confidentiality statutes, but these laws offer varying degrees of protection and many states have no laws at all. The medical profession treats improper disclosure of sensitive data as an ethical violation, but for the most part this is an unwritten and unenforceable rule. New Jersey has no specific statute governing the disclosure of medical records. New Jersey state courts have treated cases involving disputes over disclosure within a general duty of confidentiality imposed on the health care profession based on a patient's right to privacy.[142] This obligation of confidentiality applies to patient records and information, and applies not only to physicians but to hospitals as well.

9. *Other Acts Protecting Private Information*

a. *Family Educational Rights and Privacy Act Of 1974*[143]

This statute regulates the disclosure of and access to educational records, and allows students to review their records and prevent disclosure.[144]

138. 15 U.S.C. § 1666 (1994).
139. *Id.* § 1692.
140. *Id.* § 1691.
141. *Id.* § 1693.
142. *See, e.g.*, Estate of Behringer, v. Med. Ctr. 592 A.2d 1251 (N.J. 1991).
143. Pub. L. No. 93-380, 88 Stat. 571 (codified in scattered sections of 47 U.S.C.).
144. *See id.* § 513.

b. *Driver's Privacy Protection Act Of 1994*[145]

This statute makes it a criminal act for state motor vehicle offices to release driving record, age, or address information without a legitimate purpose.[146]

c. *Cable Communications Policy Act Of 1984*[147]

This act imposes restrictions on cable television systems regarding collection, use and disclosure of subscriber information, including the viewing habits of customers.[148] The cable systems must notify customers regarding information collected and may only disclose such data if the customer has first been given the opportunity to prohibit or limit such disclosure.[149]

d. *Video Privacy Protection Act Of 1988*[150]

This act prohibits the disclosure of information regarding the names of videos rented by individuals.[151] However, customer lists arranged by subject matter (but not by specific title) may be released if the customer has an opportunity to prohibit such disclosure. This law was passed after the public disclosure of Judge Robert Bork's video rental history while he was being considered for appointment to the U.S. Supreme Court.

e. *Health Insurance Portability And Accountability Act Of 1996*[152]

The main focus of this act is to regulate the health insurance industry to combat waste, fraud, and abuse. It also contains particular provisions to assure that medical information is utilized in a manner that appropriately protects the confidentiality of the information and the privacy of individuals receiving health care services and items.

---

145. 18 U.S.C. §§ 2721-2725 (1994).
146. *See id.* § 2721(a).
147. 47 U.S.C. § 551 (1994).
148. *See id.* §§ 551(b)(2)(A), (B), (c)(2)(C)(ii).
149. *See id.* §§ 551(a)(1)(A), (b)(1).
150. 18 U.S.C. §§ 2710-2711 (1994).
151. *See id.* § 2710(b)(1).
152. Pub. L. 104-191 (1996).

D. *Proposed Legislation*

1. *Medical Information Privacy And Security Act*[153]

This bill was sponsored by Senator Leahy to "provide individuals with access to health information of which they are the subject, ensure personal privacy with respect to personal medical records and health care-related information, impose criminal and civil penalties for unauthorized use of personal health information, and to provide for the strong enforcement of these rights."[154] The bill requires that persons that are the subject of protected health information be given access to that information.[155] It further requires specified parties to establish safeguards to ensure the confidentiality, security, accuracy, and integrity of protected health information; and imposes restrictions on use and disclosure.[156] The bill also establishes the Office of Health Information Privacy, specifying its duties to receive and investigate violation complaints and conduct audits.[157] Criminal and civil sanctions are imposed for violations.[158] This bill is generally more restrictive than the HHS proposals and it is likely that any final law passed will be somewhat less protective of privacy.

2. *Fair Health Information Practices Act Of 1997*[159]

This bill was sponsored by Representative Condit to establish a code of fair information practices for health information. The bill requires, subject to exceptions, health information trustees (e.g., health care providers) to permit individuals to examine their protected health information, such as physical or mental health records created or received by health care trustees.[160] Under the bill the trustees "may use protected health

153. S. 1368, 105th Cong. (1997).

154. In the 104th Congress, Senators Bennett and Leahy co-sponsored S. 1360 ("the Bennett-Leahy bill") on the topic of health information privacy. *See* S. 1360, 104th Congress (1996). This earlier bill was defeated, and Sen. Leahy now proposes this revised version. It is expected that Sen. Bennett may also propose his own separate version during the current session.

155. *See* S. 1368(I)(A) § 101(a)(1), 105th Cong. (1997).

156. *See* S. 1368(I)(B) § 111, 105th Cong. (1997).

157. *See* S. 1368(III)(A) § 301, 105th Cong. (1997).

158. *See* S. 1368(III)(B)(1) §§ 312, 312(2), 321, 105th Cong. (1997).

159. H.R. 52, 105th Cong. (1997).

160. *See* H.R. 52(I)(A) § 101(a)(1), 105th Cong. (1997).

information only for a purpose: (1) that is compatible with and directly related to the purpose for which the information was collected or received by the trustee;" or (2) for which the trustee has received disclosure authorization.[161] The bill does make exceptions regarding: (1) next of kin and directory information; (2) public health; (3) health research; (4) emergencies; (5) judicial and administrative purposes; (6) law enforcement; and (7) subpoenas, warrants, and search warrants.[162]

3. *Consumer Internet Privacy Protection Act of 1997*[163]

This bill was sponsored by Representative Vento to prohibit interactive computer services from disclosing "to a third party any personally identifiable information provided by a subscriber without the subscriber's informed written consent."[164] The bill permits the subscriber to revoke such consent at any time and requires the service to cease disclosing such information, and permits enforcement by private civil actions.[165] The bill also requires, at a subscriber's request, interactive computer services to: (1) provide the individual with his or her personally identifiable information maintained by the service; (2) permit the subscriber to verify and to correct such information; and (3) provide to the subscriber the identity of the third party recipients of such information.[166] The FTC is also granted the authority to: (1) investigate whether a service has been or is engaged in any act or practice prohibited by this Act; and (2) if so, issue a cease and desist order as if such service were in violation of specified provisions of the Federal Trade Commission Act.[167]

4. *Federal Internet Privacy Protection Act Of 1997*[168]

This bill was sponsored by Representative Barrett and prohibits any Federal agency from making available through the Internet any record with respect to an individual.[169] The bill

161. H.R. 52(I)(B) § 111(a)(1), (2), 105th Cong. (1997).
162. *See* H.R. 52(I)(B) §§ 114-120, 105th Cong. (1997).
163. H.R. 98, 105th Cong. (1997).
164. *Id.* § 2(a)(1).
165. *See id.* § 2(a)(2).
166. *See id.* §§ 2(c)(1)(A), (B).
167. *See id.* § 3(b)(1).
168. H.R. 1367, 105th Cong. (1997).
169. *See id.* § 2(a).

permits a civil action to be brought against an agency by an individual suffering harm as a result of any case in which an agency makes available through the Internet a record with respect to the individual (including a case in which a record was made available through the Internet before enactment of this Act).[170]

5. *Communications Privacy And Consumer Empowerment Act*[171]

This bill was re-introduced by Representative Markey to require the FTC to determine ways for consumers to stop unauthorized on-line use of personal information.[172] The bill directs the FCC to assess whether ISPs adequately protect against unauthorized interception of communications and personal information.[173] It requires ISPs to offer customer screening software designed to limit access to material that is inappropriate for children.[174] Finally, it "prohibits the Federal Government or State governments from: (1) restricting or regulating the sale in interstate commerce of encryption or other products for improvement of data security; (2) conditioning the issuance of certificates of authentication or authority upon any escrowing or sharing of private encryption keys; or (3) establishing a licensing or other regulatory scheme that requires key escrow as a condition of regulatory approval."[175]

6. *Social Security On-Line Privacy Protection Act*[176]

This bill was sponsored by Representative Franks to prohibit an ISP from disclosing SSNs or related personal information without prior written consent.[177] It requires the ISP to permit an individual to revoke any consent at any time, upon which revocation the ISP shall cease disclosing such number or

170. *See id.* § 2(b).
171. H.R. 1964, 105th Cong. (1997).
172. *See id.* § 101.
173. *See* H.R. 1964(I) § 102(2), 105th Cong. (1997).
174. *See id.* § 103.
175. H.R. 1964(II) § 203, 105th Cong. (1997).
176. H.R. 1287, 105th Cong. (1997).
177. *See id.* § 2(a).

information to a third party.[178] Under this bill, the Federal Trade Commission has enforcement authority.[179]

7. *Internet Freedom And Child Protection Act Of 1997*[180]

This bill was sponsored by Representative Lofgren to repeal restrictions on transmitting obscene materials to minors using telecommunications or computer equipment.[181] The bill requires an ISP to offer customer-screening software to limit access to material that is unsuitable for children.[182]

8. *Unsolicited Commercial E-Mail Choice Act Of 1997*[183]

This bill was sponsored by Senator Murkowski to require a person who transmits unsolicited commercial e-mail to prominently display the word "advertisement" along with the sender's name, e-mail address, and phone number.[184] The bill will not be applied to ISPs unless it was the ISP that initiated the transmission. Consumer requests for termination of unsolicited mail must be honored within 48 hours. The bill empowers the FTC with regulatory authority over such unsolicited e-mail, although the bill authorizes a private right of action within 1 year after receipt of the transmission.[185]

9. *Electronic Mailbox Protection Act Of 1997*[186]

This bill, which was sponsored by Senator Torricelli, levies a $5,000 civil penalty on any person who transmits an unsolicited e-mail message and uses a technical procedure to disguise the source.[187] It applies to senders who fail to comply with the request of the recipient to cease sending e-mail messages.[188]

178. *See id.* § 2(b).
179. *See id.* § 3(b).
180. H.R. 774, 105th Cong. (1997).
181. *See id.*
182. *See id.* § 2(d)(1).
183. S. 771, 105th Cong. (1997).
184. *See id.* § 3(a)(1).
185. *See id.* §§ 4(a), 8(a).
186. S. 875, 105th Cong. (1997).
187. *See id.* § 3(a).
188. *See id.* § 3(a)(3).

The bill empowers the FTC with regulatory authority over such unsolicited e-mail.[189]

10. *Netizens Protection Act Of 1997*[190]

This bill is sponsored by Representative Chris Smith (R-NJ) and was introduced on May 22, 1997.[191] The bill, which is actually an extension of the Telephone Consumer Protection Act of 1991,[192] created a cause of action against "junk faxes."[193] The bill extends the protection against junk faxes to unsolicited commercial e-mail or "spam," essentially creating a scheme through which potential recipients must "opt-in" to receiving unsolicited commercial e-mail.[194]

E. *Common Law And State Statutes*

1. *Privacy Torts*

Tort law is a traditional means of redressing violations of privacy interests in the private sector, as discussed in the Restatement (Second) of Torts.[195] In particular, employee privacy is recognized as a protected interest under state common law. In the context of e-mail and on-line privacy, there are four torts of potential importance.

a. *Intrusion Upon Seclusion*

This tort creates liability against one who intentionally intrudes (physically or otherwise) upon the seclusion of another or his private affairs where such intrusion would be highly offensive to a reasonable person.[196] Electronic means of intrusion would fall within the ambit of this tort. Actions here could be brought regarding access to private communications (e-mail), and intrusion via junk e-mail.
This tort is limited in that:

189. *See id.* § 3(b).
190. H.R. 1748, 105th Cong. (1997).
191. *See id.*
192. Public Law 102-243, 102nd Cong. (1991).
193. *See* 47 U.S.C. § 227(3) (1994).
194. *See* H.R. 1748 § 2(3)(1), 105th Cong. (1997).
195. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977).
196. *See id.* § 652B.

the action must be intentional so that accidental access to e-mail would not give rise to liability;

the matter must be "private" such that the plaintiff would need to show a reasonable expectation of privacy;

the intrusion must be "highly offensive"; and

in the employee setting, pre-established consent (including an announced employer policy of non-privacy of all e-mail communications) would work as a defense.

The few cases based on this tort in the employee e-mail context have dismissed the claim and are summarized as follows:

Flanagan v. Epson America Inc[197] - In this case, employees claimed that a tap on the company's e-mail system violated their expectation of privacy when their messages were read and printed without consent.[198] The court held for the defendant company because California does not recognize e-mail as a type of communication afforded privacy protection.[199] Other California cases in accord are *Shoars v. Epson America Inc.*[200] and *Bourke v. Nissan Motor Co.*[201]

Smyth v. Pillsbury Co.[202] - In this case, an employee claimed an invasion of privacy when his e-mail messages were read and printed after he was repeatedly assured that such communications were to be kept confidential and privileged.[203] The employee was fired after sending messages concerning the sales staff, containing threats to "kill the back-stabbing bastards."[204] In interpreting Pennsylvania law, the federal court found no reasonable expectation of privacy in messages voluntarily communicated over the company e-mail system, regardless of any assurances of confidentiality.[205] The court also found that the employer's interception of such messages was not offensive, and that the company's

197. No. BC 007036, slip op. (Cal. App. Dep't Super. Ct. Jan. 4, 1991).

198. *See id.*

199. *See id.*

200. No. BO73234, slip op. (Cal. Ct. App.), review denied, No. SO40065, 1994 Cal. LEXIS 3670 (June 29, 1994).

201. No. YC 003979, slip op. (Cal. App. Dep't Super. Ct. 1991).

202. 914 F. Supp. 97 (E.D.Pa. 1996).

203. *See id.* at 98.

204. *Id.* at 98, n.1.

205. *See id.* at 99.

interest in preventing unprofessional comments outweighed any privacy interest on the part of the employee.[206]

b. *Publicity Given To Private Life*

This tort creates liability against one who gives publicity to private, personal information if the disclosure would be highly offensive to a reasonable person, and if the matter is not of legitimate public concern.[207] Like defamation, this tort is limited by First Amendment concerns regarding the freedom of speech and press to publicize true facts. Since publicity in this context essentially means disclosure to a large number of people, dissemination of private information via the Internet would qualify. The tort is limited in that the matter must be private and the behavior offensive as noted above.

c. *Placing A Party In A False Light*

This tort creates liability against one who gives publicity to a matter concerning another that places the other in a false light if the false light would be highly offensive to a reasonable person, and if the actor had knowledge of or acted in reckless disregard as to the falsity.[208] This tort could be applied to misinformation published on the web subject to the offensiveness and scienter limitations.

d. *Right Of Publicity*

This tort creates liability against one who appropriates, to his own use or benefit, the name or likeness of another.[209] It is recognized that one has a privacy interest in the exclusive use of his own identity. This interest is restricted however, when inconsistent with First Amendment principles, as when a newspaper publishes the name or photograph of someone in connection with a newsworthy event.[210] This principle was tested in the on-line context in *Stern v. Delphi Internet Servs. Corp.*,[211]

206. *See id.* at 101.
207. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).
208. *See id.* § 652E.
209. *See id.* § 652C.
210. *See* Stern v. Delphi Internet Servs. Corp., 626 N.Y.S.2d 694 (Sup. Ct. N.Y. County 1995).
211. 626 N.Y.S.2d 694 (Sup. Ct. N.Y. County 1995).

where radio personality Howard Stern sued the Delphi system for using his photograph without permission in an advertisement for an on-line debate regarding Stern's candidacy for governor of New York.[212] The court held for Delphi on First Amendment grounds because of the newsworthy quality of the event.[213]

2. *Intentional Infliction Of Emotional Distress*

This tort might be applicable in the employment context where an employer intentionally or recklessly caused severe emotional distress to the employee by extreme and outrageous conduct.[214] However, liability here would only seem to attach in extreme situations. Ordinary employer monitoring of an employee's communications on an employer-owned system would not likely constitute "outrageous" conduct. Misuse or threatened unprivileged dissemination of acquired information or more extensive monitoring of personal messages than the business purpose requires would need to be shown. Further, the employee would have to show actual injury in order to establish employer liability.

3. *Conversion*

The tort of conversion has been recognized in the on-line context in the case of *Compuserve, Inc. v. Cyber Promotions*,[215] where the excessive storage of junk e-mail on CompuServe's computers represented a "taking."[216] In relation to ordinary consumers, forced downloading of junk e-mail and files that is paid for by the consumer in access fees may also be actionable.

4. *Trade Secret Laws*

A tort action will lie for misappropriation of trade secrets if there is an actual trade secret, and if there is either a breach of confidence regarding that secret or the secret is accessed by improper means.[217] The first element requires that information be

212. *See id.* at 695.
213. *See id.* at 700.
214. *See* RESTATEMENT (SECOND) OF TORTS § 46 (1977).
215. 962 F. Supp. 1015 (S.D. Ohio 1997).
216. *See id.* at 1020.
217. *See* RESTATEMENT (FIRST) OF TORTS § 757 (1977).

kept secret where the owner has taken sufficient measures to maintain that secrecy.[218] If a company's private information is communicated by businesses on-line, then the company must take steps (e.g., encryption) to protect it. A company might also form an agreement with an ISP regarding the secrecy of its data kept within an ISP database. Under such a confidential relationship, the ISP would be liable for damage to the company if the data were disclosed. A trade secret claim could also be made against any hacker that damaged a company through gaining unauthorized access to its data.

5. *New Jersey Wiretapping Statute*[219]

Most states have enacted wiretap statutes that provide comparable protection to that of the ECPA. State statutes are generally not preempted by the ECPA if they afford greater privacy protection than the ECPA. As such, it is possible for activities of ISPs and employers that are exempt under the ECPA to, nevertheless, create liability under state statutes. However, privacy protection under these statutes is generally not much greater than that afforded by the ECPA. In fact, New Jersey has a provision expressly favoring law enforcement, which provides that a court order may require ISPs to create and release backup copies of private communications for preservation as evidence.[220]

V. Self Regulation

A. *The Industry View*

Beyond legal regulation of privacy issues, non-mandatory guidelines and self-interest may provide a framework for privacy protection in the on-line world. Government intervention may not be the appropriate solution because of the difficulty of keeping laws current with the technology and because of the possibility of inhibiting technological and commercial progress. In support of this view, the industry has argued that market pressures will force self-regulation regarding privacy of information as users make their privacy preferences known. In light

218. *See id.*
219. N.J. STAT. ANN. § 2A:156A (et seq.) (West 1998).
220. *See id.* § 2A:156A-12.

of the universal interest in promoting the benefits of networking technology, it is argued that ISPs, employers and other players will not engage in activity that is so invasive as to frustrate use of e-mail and other systems.

B. *The Privacy View*

In opposition to the industry view, privacy advocates argue that in light of the actual privacy violations that have already occurred, self-regulation has already failed.[221] The argument is further made that, under non-mandatory guidelines, companies that respect privacy and adhere to guidelines will be at a competitive disadvantage in comparison to those that do not. AOL's changed privacy policy (as previously discussed) may be an indication that industry's self-regulation is on the decline, causing concern for on-line users.

VI. *Self-Help*

Many individuals and businesses are turning to self-help approaches for solving their privacy and security needs. While the primary technique of ensuring the confidentiality of e-mail information is encryption, other means of hiding identity and transactional information are also in use.

A. *Encryption*

Encryption has long been employed by the military to secure information from hostile forces. But with the advent of ubiquitous digital communications in the commercial world has also come readily available and extremely powerful encryption software that rivals the effectiveness of military capabilities. The strong encryption schemes are for all practical purposes "unbreakable."

1. *Symmetrical Encryption*

This type of encryption has been in use since ancient times. The approach here is that a sender uses a particular code key to encrypt a message. The receiver must be in possession of the same key to de-encrypt the message. The problem with this

221. Such privacy advocates include the Center for Democracy and Technology (CDT) and the Electronic Privacy Information Center (EPIC).

scheme is that it is impractical to distribute a confidential key to more than a small number of trusted parties. The U.S. military has used this approach under the Defense Encryption Standard in conjunction with complex key management schemes to control how keys are transmitted and/or distributed to maintain the integrity of the system.

2. *Asymmetrical Encryption*

A more recent approach is asymmetrical encryption whereby separate private and public keys are used to encrypt and decrypt messages. Although the private and public keys are mathematically related, knowledge of one is insufficient to allow computation of the other. With asymmetric encryption, the sender will use a private key to encrypt a message that may only be de-encrypted with the corresponding public key possessed by the receiver. The private key must be kept confidential and is only possessed by its owner. In contrast, the public key may be possessed by anyone because it is of no value, except as the complement to the private key. A potential flaw in this scheme is that individuals using the public key need to be assured that this key is indeed associated with the bona fide sender and not an impostor. One solution is to employ trusted Certification Authorities (CA) that can vouch for and verify the binding between public keys and their proper owners. There are a number of commercial software packages, such as Secure Messenger, RSA, PGP and Viacrypt that provide asymmetrical encryption capabilities. In addition, companies like Verisign and GTE are providing CA services.

3. *Confidential Communications On The Internet*

The use of encryption to ensure confidentiality is of special concern for attorneys because of their special ethical responsibilities. Specific considerations that should be weighed by attorneys in deciding to communicate without encryption over an unprotected network (such as the Internet) include possible ethics violations, malpractice, compromised reputation with clients, waiver of the attorney-client privilege, and loss of client trade secret protection.

VII. Legislation

A. *Current U.S. Policies*

In the United States, until December 1996, the export of cryptographic products was controlled by the Department of State via the Arms Export Control Act[222] under the department's International Traffic in Arms Regulations (ITAR).[223] Under ITAR, no cryptographic product could be exported without an export license issued by the Department of State, and licenses were generally not granted for products that provide "strong" encryption (e.g., greater than 40 bit codes).[224] However, on November 15, 1996 under Executive Order 13026,[225] President Clinton transferred the responsibility for control of export of cryptographic products to the Department of Commerce.[226] To this end, the President amended the Export Administration Regulations (EAR)[227] as part of a plan to implement a worldwide key management infrastructure featuring key escrow and key recovery provisions. To allow a transition period for the development of this key management infrastructure, if an exporter makes satisfactory commitments to build and/or market recoverable encryption items and to help build the supporting international infrastructure, the present EAR rule permits the export and re-export of 56-bit key length Defense Encryption Standard or equivalent strength encryption items under the authority of a License Exception.[228] This policy applies to both hardware and software. Both privacy and electronic commerce advocates are now calling for legislation to change these restrictive policies.

1. *U.S. Government Clipper Initiatives*

In the face of inexpensive commercial encryption packages that are essentially bulletproof, law enforcement has argued that its ability to control crime will be seriously degraded. Therefore, the "Clipper" initiatives have been proposed as a

222. 22 U.S.C. §2778 (1996).
223. *See* 22 C.F.R. pts. 120-130 (1998).
224. *See* 22 U.S.C. § 121.1 category XI(b)(1) (1996).
225. 32 WEEKLY COMP. PRES. DOC. 2399 (1996).
226. *See id.* § 1.
227. 15 C.F.R. § 730 et seq. (1996).
228. *See id.*

means of implementing private security while at the same time allowing law enforcement to decrypt secure data for legitimate purposes. Over time, three different plans have been proposed:

a. *Clipper I*

This was a 1993 proposed hardware solution where communications would be uniquely identified using keys permanently embedded in hardware (i.e., the clipper chip). This was intended to provide a "back door" to government to permit legitimate eavesdropping of otherwise confidential communications.

b. *Clipper II*

This was a 1995 proposed mandatory Commercial Key Escrow (CKE) framework for public key encryption that would allow businesses to select their own encryption algorithms, but which also would provide the government with means to gain access to encrypted data.

c. *Clipper III*

This is also called the Electronic Data Security Act of 1997 draft legislation, and is a proposal for a Key Management Infrastructure (KMI) for public key encryption whereby private CA and key escrow entities would operate under government policies. To participate in the system, users would have to make sure their private keys were deposited with trusted agents that would be permitted to release the keys to the government for purposes of law enforcement. To date, none of the Clipper proposals have been formally approved or made mandatory in the commercial sector. Conformance with Clipper policies is only mandatory at present for contracts with government.

2. *Secure Public Networks Act*[229]

This bill was sponsored by Senator McCain to allow the use of any encryption desired, except as otherwise provided by the bill or by law.[230] The bill would prohibit the Federal Government or a State from requiring the escrow of an encryption key

229. S. 909, 105th Cong. (1997).
230. *See id.* § 101.

with a third party.[231] Key recovery agents would be required to disclose recovery information to government for specified lawful purposes.[232] Regarding the export of encryption, the Secretary of Commerce is granted "jurisdiction over the export of commercial encryption products and the sole duty to issue export licenses on such products."[233] The President is authorized to increase the encryption strength for products permitted to be exported. The bill criminally prohibits export "if the Secretary finds that a product would be: (1) used in acts against the national security, public safety, transportation systems, communications networks, or essential systems of interstate commerce; (2) diverted to a military, terrorist, or criminal use; or (3) reexported without authorization."[234]

3. *Security And Freedom Through Encryption (SAFE) Act Of 1997*[235]

This bill was sponsored by Representative Goodlatte and is intended to relax federal governmental export controls on encryption.[236] Several amendments have been proposed. The original Goodlatte language has been substantially amended by five House committees to provide law enforcement with easy access to encrypted information. Representative Solomon (R-NY), chairman of the House Rules Committee, has indicated that he will not send the legislation to the House floor unless it contains domestic controls providing law enforcement access.

4. *Encrypted Communications Privacy Act Of 1997*[237]

This bill was sponsored by Senator Leahy to allow any person to make non-criminal use of encryption, regardless of algorithm or key length.[238] The bill prohibits Federal or State Government from requiring that a decryption key be given to another person.[239]

---

231. *See* S. 909(I) § 102, 105th Cong. (1997).
232. *See id.* § 106.
233. S. 909(III), 105th Cong. (1997).
234. *Id.* § 306.
235. H.R. 695, 105th Cong. (1997).
236. *See id.*
237. S. 376, 105th Cong. (1997).
238. *See id.* § 5(a).
239. *See id.* § 5(b).

5. *Computer Security Enhancement Act Of 1997*[240]

This bill was sponsored by Representative Sensenbrenner to amend the National Institute of Standards and Technology Act to require NIST to: (1) "assist in establishing voluntary interoperable standards" and guidelines to facilitate the establishment of non-Federal public key management infrastructures that can be used to conduct transactions with the Federal Government;[241] and (2) provide assistance to Federal agencies in the protection of computer networks.[242] The bill was passed in the House and is under consideration by the Senate.

6. *Promotion of Commerce On-Line In The Digital Era (Pro-CODE) Act Of 1997*[243]

This bill was sponsored by Senator Burns to prohibit the Secretary of Commerce (acting through NIST or otherwise) from promulgating or enforcing regulations, or otherwise carrying out policies that: (1) result in encryption standards intended for use by businesses or entities other than Federal computer systems;[244] or (2) have the effect of imposing Government-designed encryption standards on the private sector by restricting the export of computer hardware and computer software with encryption capabilities.[245]

B. *Pseudonyms*

To protect their interest in anonymity, on-line users frequently use pseudonyms in making public statements. Many ISPs allow users to adopt pseudonyms in "signing" public messages posted on the electronic bulletin boards provided by the ISP. Although laudable in its promotion of free speech, this practice has unfortunately been abused by some users in perpetrating child pornography, defamation and copyright infringement.

240. H.R. 1903, 105th Cong. (1997).
241. *See id.* § 3(2).
242. *See id.* § 4.
243. S. 377, 105th Cong. (1997).
244. *See id.* § 4(a).
245. *See id.* § 4(b).

C. *Anonymous Remailers*

Anonymous remailers are special on-line services that receive messages from users, strip their identifying information and then forward them to their intended destination. In this case, the source of the message can only be traced back to the remailer and not to the original sender. This provides the same free speech benefits as pseudonyms with the same dangers for abuse.

D. *Use Of Digital Cash*

One of the primary benefits of using ordinary cash in a commercial transaction is the fact that it cannot be traced back to the purchaser. "Digital cash" schemes are now being used to provide this same privacy attribute. Although it might appear as though the only people with a real need for the ability to spend anonymously are criminals, this is not really true. It is also desirable to many people to be able to conduct anonymous transactions in the interest of protecting a variety of personal data, a privacy interest already compromised in the context of credit card purchases.

E. *ISPs, Firewalls, The Anonymizer, And Cookie Killers*

If a user accesses the Internet through an ISP such as AOL, CompuServe and others, the ISP's proxy server acts as an intermediary to protect the user's identity and e-mail address. Web sites that attempt to trace the user's location will only be able to do so as far as the proxy server. In this case, only the ISP could trace the user's "clickstream" data. Intranets that are protected by firewalls will likewise provide this same protection. A firewall is a piece of software operating on the computer that acts as the gateway from a private network to the Internet. The firewall software provides an intelligent "filter" between networks that monitor message traffic and screen out unauthorized data.

The Anonymizer is a special web service that may be used to block web sites from collecting user information.[246] The user simply goes to that site, and then makes all subsequent links from there. It prevents collection of source and other data, or

246. *See Anonymizer, Inc. - Comprehensive identity privacy and anonymity services* (visited Oct. 24, 1998) <http://www.anonymizer.com>.

the introduction of cookies onto the user computer. The only disadvantage is that it will slow down the access time involved in surfing from site to site. The Anonymizer also provides a sample service whereby it can display to you the type of information that can be collected as a result of your visiting that site. For example, it may display your site provider, approximate geographic location, and browser type.

There are also software programs available to control the placement of cookies on a user's computer. As mentioned, browsers such as Netscape and Internet Explorer allow users to set options to provide notice when a web site is attempting to place a cookie. Further, there are programs such as "Cookie Cutter," "Cookie Crusher," and "Cookie Master" that both permit removal of existing cookies and prevent the placement of new cookies.

VIII. Other Means to Enhance Privacy

A. *Universal Registration Systems (I/Code system)*

This is a system proposed by the Internet Profiles Corporation where users register personal data with the I/Code system and then receive a unique identifier that allows anonymous browsing. This approach attempts to protect both privacy and market interests in that anonymity is protected, while aggregate demographic information may still be collected for marketing analysis. The aggregate data could not, however, be traced to an individual.

B. *Cookies*

A use beneficial to privacy has actually been proposed for the much-maligned "cookie." Instead of being used as an information-gathering tool, a cookie could be used to store privacy preference data. Once the user communicated his privacy preference to the web site, the site would honor requests for consent and notice regarding collection of information. The only catch here is that voluntary compliance by the web site would be required. Another beneficial effect of cookies is to prevent exposure to unwanted or repetitious advertising. Since the cookie stores user preference information, it may be used to filter ad-

vertisements that are irrelevant to the user or to keep track of whether a given advertisement has already been viewed.

C. *Platform For Internet Content Selection (PICS)*

This system was initially developed by the WWW Consortium at MIT for the purpose of allowing parents to block children's access to sites that were deemed "objectionable" in terms of pornographic, violent or hateful content. Under this approach, when a user attempts to access a given web site, the PICS software first checks with a central database to determine if the site has been marked as "objectionable." If so, the user's access to the site will be blocked. However, because the system itself is "viewpoint neutral," it could also be used to rate sites regarding the privacy protections that they make available. Using this system, those sites not listed as secure would be blocked from access. Like any censoring approach, PICS is however subject to abuse in the "ratings" system.

IX. Conclusion

The problems involved in maintaining personal privacy will continue to be issues of debate and dispute and the impetus for new laws in the foreseeable future. As society progresses further into the information age, personal data will be collected and exploited at an ever-expanding rate. In addition, the technological means to accomplish this will continue to evolve at a pace that will challenge and perhaps confound the legal profession. Our present privacy laws, already out of date, will be further stretched and likely made even less effective in providing protection. As seen, laws like the ECPA have already been severely weakened by on-line communications technology. For example, because the ECPA allows access to stored communication, this means from a practical perspective that all e-mail is accessible by employers and ISPs. Other legal approaches such as tort law have been held to provide little, if any, protection. At least from the communications perspective, the self-help remedy of public key encryption appears to be the best near term solution to privacy concerns. Efforts to limit domestic encryption thus far have failed, and a number of effective and inexpensive software and service packages are now available. The strong societal interest in fostering electronic commerce

will likely cause continued support for and a ubiquitous presence of encryption. However, law enforcement will continue to demand a means for access to encrypted data as no satisfactory compromise with privacy advocates has yet been proposed. Threats to privacy of personal information are not easily solved by self-help, and further legal protection is needed. While the PPA and the proposed Consumer Internet Privacy Protection Act are steps in the right direction, stronger regulation must still be considered. Given the propensity and incentives for entities to probe into the personal affairs of the private individual, the need for protection will continue to be critical. The very existence of web sites such as "The Stalker's Home Page" make this point abundantly clear.[247]

X. Sample Policies for Control of Computer Information, Voice Mail, E-mail and the Internet

A. *Sample Policy: Introduction*

Employee privacy does not extend to work-related conduct or to the use of company-provided facilities such as computers.

Use of any of the Computer Systems in violation of any of the policies herein will result in disciplinary action, up to and including termination.

B. *Prohibited Uses and Communications*

Computer Systems are not to be used to send or store any material of a personal character, other than occasionally and incidentally. The following types of communication are strictly prohibited:

Gossip, personal attacks, or embarrassing remarks;
Personal information about yourself or others;
Profanity or obscenity in any form;
Insensitive language which is derogatory, offensive, threatening, insulting or harmful to morale; and
Sexually-explicit messages, cartoons, or jokes; unwelcome propositions or love letters; ethnic or racial slurs.

247. *See The Stalker's Home Page — No More Privacy! — As Seen on the LEEZA Show* (visited Oct. 24, 1998) <http://www.glr.com/stalk.html>.

C. *Monitoring of Computer Systems*

All messages sent and received by the computer systems or information stored in the computer systems are Company records.

The Company reserves the right to access and disclose all such messages and information for any business purpose.

Employees should ensure that messages sent, received, and stored on Company business or with the use of Company facilities will be available for review without prior notice.

All passwords and encryption keys must be available to management.

You should not use the computer for the communication or storage of anything you would not want read and further disclosed.

D. *Internet Policy: Permitted Uses*

E-mail for business purposes of the Company;

Support of Company customers in their use of Company services;

Reading and downloading legitimate business data and information; and

Downloading bug fixes and patches for authorized commercial software.

E. *Internet Policy: Prohibited Uses*

for any unlawful activity;

to make any defamatory remarks, or derogatory remarks based on race, religion, color, sex, handicap, or national origin;

for distribution, disclosure or selling of proprietary information;

to download or distribute any copyrighted material without license to do so;

to advocate a religious or political cause;

to promote any commercial enterprise other than approved Company business;

for an employee's off-the-job pursuits, whether or not commercial in nature;

for sending or soliciting sexually oriented messages or images;

to seek employment;

to send viruses or to do any act harmful to another person or his computing resources;

to send "junk" mail or "spamming" e-mail;

to entrust confidential company information, such as trade secrets or proprietary information, to this medium without prior permission.