Boston University
Journal of Science & Technology Law

Article

Marginalizing Individual Privacy on the Internet

Deborah M. McTigue

Table of Contents

Marginalizing Individual Privacy on the Internet*

Deborah M. McTigue†

I. INTRODUCTION

1. Many Internet users are under the delusion that their Internet conversations are private. While you may that think your computer is "your own private peephole into cyberspace, . . . [i]t turns out the peephole is a two-way viewer. Some of the Internet's defining characteristics—high-tech tricks and search methods that make finding information easy—allow others in cyberspace to take a peek at your behavior."[1]

2. Users generally access the Internet through an Internet Service Provider ("ISP"), using Netscape Navigator, Microsoft Internet Explorer, or a proprietary browser such as America Online ("AOL"). ISPs generally offer e-mail services and many employers also provide their employees with access to the Internet and e-mail. Like commercial ISPs, employers store employee e-mail on company-owned central computers until users download it to their personal computers. Many corporations and private individuals also publish World Wide Web ("Web") pages that invite e-mail correspondence, display advertising, or offer online purchasing.

3. When an individual visits a Web site, makes a purchase, or sends e-mail, a stream of personal data may be recorded. Even if a user is careful, "[y]our machine has been spreading information about you and your browsing habits . . . [b]y sharing cookies."[2] A "cookie" is a file that is downloaded and uploaded from a computer's hard drive. Cookie files store information about the sites a user visits and may include "your full name, address, telephone number, fax number and e-mail address."[3] Although users can delete cookie files from their computers' hard drives, ISPs and employers also store cookie files and generally do not permit access to these storage devices.

 Cite to this Article as 5 B.U. J. SCI. & TECH. L. 5 (1999). Pin cite using the appropriate paragraph number. For example, cite to the first paragraph of this Article as 5 B.U. J. SCI. & TECH. L. 5 para. 1 (1999).

† B.A., with honors, University of Florida, 1976; J.D., *summa cum laude*, valedictorian, Nova Southeastern University, Shepard Broad Law Center, 1998. Ms. McTigue is an associate with the law firm Ruden, McClosky, Smith, Schuster & Russell, P.A. in Fort Lauderdale, Florida.

[1] Rebecca Quick, *Don't Expect Your Secrets to Get Kept on the Internet: Privacy Is Always at Risk As You Surf*, WALL ST. J., Feb. 6, 1998, at B5.

[2] Mike West, *Privacy on the Net: Who's Minding the Cookie Jar?*, 6 N.J. LAW.: WKLY. NEWSPAPER 1356, 1356 (1997).

[3] *Id*.

4. In addition to deleting cookie files from their personal computers, users may rely on federal statutes, contractual agreements, or common law remedies to defend against invasions of their privacy. Relying on these protections may be insufficient, however, in a computing environment having a multitude of users. To illustrate this problem, this Article discusses various situations that exhibit an increasing trend of marginalization of individual privacy on the Internet. Part II discusses online privacy in relation to ISPs. Part III explores employees' expectations of privacy in company e-mail and employers' needs to protect business records, which are discoverable during litigation. Part IV examines the attorney-client privilege in relation to electronic communications. Finally, Part V reviews current congressional and industrial developments aimed at increasing online privacy.

II. PRIVACY AND ISP OPERATORS

5. ISPs are central to the issue of Internet privacy. Most individuals send e-mail or access the Internet from their homes via a commercial ISP. ISP operators may only disclose the contents of an electronic communication, a record, or other information pertaining to a subscriber in accordance with the Electronic Communications Privacy Act ("ECPA").[4] The ECPA protects subscribers' privacy rights against unauthorized governmental intrusion or ISP disclosures.[5] In spite of this statutory protection and the contractual agreements that subscribers and ISPs may enter into, a subscriber's reasonable expectation of privacy may be based on a false perception of security and cyberspace anonymity.

A. Don't Ask, Don't Tell

6. Unlike the convicted Oklahoma City bomber who happens to share his name, retired officer Timothy McVeigh "is a highly decorated seventeen-year veteran of the United States Navy who has served honorably and continuously since he was nineteen years old."[6] McVeigh's career spiraled downward, however, when the Navy sought to discharge him under the statutory policy known as "Don't Ask,

---

[4] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. §§ 2510-21, 2701-10, 3121-26 (1994)). This Article focuses primarily on Title II - Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-10.

[5] *See* LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 170-71 (1995).

[6] McVeigh v. Cohen, 983 F. Supp. 215, 217 (D.D.C. 1998) ("At the time of the Navy's decision to discharge him, he was the senior-most enlisted man aboard the United States nuclear submarine U.S.S. *Chicago*").

Don't Tell, Don't Pursue."[7] Under this policy, the military may discharge service persons that say they are gay, engage in homosexual conduct, or try to marry someone of the same sex.[8]

7. McVeigh came to the Navy's attention when a civilian Navy volunteer received an e-mail message from the AOL screen name "boysrch."[9] The volunteer used the AOL member profile directory and found out that the sender was another AOL subscriber named "Tim," who worked in the military and identified himself as gay.[10] The profile included hobbies such as "collecting pics of other young studs" and "boy watching."[11] The profile did not include specific information, however, such as a last name, address, or telephone number, that could directly link McVeigh to the message.[12] Despite the anonymous nature of the profile, the volunteer suspected that McVeigh authored the message,[13] so she forwarded the information to personnel aboard McVeigh's submarine.[14]

8. A member of the Navy's Judge Advocate General asked a paralegal to contact AOL and find information about "Tim" without a warrant or court order.[15] The paralegal called AOL and pretended that he had received a fax from an unknown source.[16] An AOL representative disclosed that McVeigh was the customer behind the message.[17] Initially, AOL personnel denied the disclosure, stating that "there are so many levels to safeguard privacy that the conversation the Navy describes could not have taken place — and there is no evidence that it

---

[7] *See id.* at 217-18 (citing 10 U.S.C. § 654(b)(2) (1994) ("A member of the armed forces shall be separated from the armed forces under regulations prescribed by the Secretary of Defense if . . . the member has stated that he or she is a homosexual or bisexual, or words to that effect . . . .")).

[8] *See Morning Edition* (NPR radio broadcast, Jan. 13, 1998), *available in* 1998 WL 3306037; *see also* 10 U.S.C. § 654(b)(2).

[9] *See* McVeigh, 983 F. Supp. at 217.

[10] *See id.*

[11] *Id.*

[12] *See id.*

[13] *See id.* (stating that McVeigh's message concerned a toy-drive the volunteer was coordinating, about which she had previously corresponded with McVeigh).

[14] *See id.*

[15] *See id.*

[16] *See id.*

[17] *See id.*

did."[18] Following an investigation, the Navy told McVeigh that he was "'suspected of sodomy and indecent acts.'"[19] Although McVeigh argued that the word "gay" in his profile was insufficient to prove the Navy's allegations, he was separated based on his "propensity to engage in homosexual conduct."[20] At a subsequent administrative discharge hearing, the Navy ruled against McVeigh, finding that his online profile violated the Navy's policy on homosexuality.[21]

9. To stay his pending discharge, McVeigh sought a preliminary injunction in federal court.[22] McVeigh asked the court to find that he had not violated the "Don't Ask, Don't Tell, Don't Pursue" policy because he did not "tell."[23] Additionally, McVeigh claimed that the Navy impermissibly "asked and zealously pursued" confidential information stored in AOL customer files.[24] The court found McVeigh's argument persuasive and held that his e-mail did not amount to a statutory violation of the Navy's policy.[25] The court stated that "[s]uggestions of sexual orientation in a private, anonymous email account did not give the Navy a sufficient reason to investigate to determine whether to commence discharge proceedings."[26] The court also noted that "in the context of cyberspace, a medium of 'virtual reality' that invites fantasy and affords anonymity, the comments attributed to McVeigh do not by definition amount to a declaration of homosexuality."[27]

10. The court also held that McVeigh's claim would likely succeed on the merits because there had been a violation of the ECPA, which was "enacted by

---

[18] Elaine Herscher, *Discharge for Online Gay Profile: Sailor Says Navy Got Info Improperly*, S.F. CHRON., Jan. 10, 1998, at A3, A5.

[19] *Id*.

[20] *Id*. "If the U.S. Navy is allowed to fire someone based on information illegally obtained from AOL, then who's next? . . . Can a private company call AOL to investigate an employee and then fire him?" *Id*. (quoting John Aravosis, an Internet political consultant).

[21] *See* McVeigh, 983 F. Supp. at 218.

[22] *See id*. at 216.

[23] *See id*. at 218.

[24] *See id*.

[25] *See id*. at 219 (noting that McVeigh's profile did not cross the statutory threshold required to investigate because it amounted to no more than "an abstract preference or desire to engage in sexual acts").

[26] *Id*.

[27] *Id*.

Congress to address privacy concerns on the Internet."[28] The ECPA provides that the government may acquire information from an ISP only if it obtains a warrant or notifies the subscriber and issues a subpoena or obtains a court order.[29] The government argued, however, that the statutory language in § 2703(c) of the ECPA placed "an obligation on the online service provider to withhold information from the government, and not vice versa."[30] Thus, under the government's interpretation, McVeigh would not have a cause of action against the Navy, because § 2703(c) was a prohibition aimed at AOL.

---

[28] *Id*.

[29] *See id*. (citing 18 U.S.C. § 2703(b)(1)(A)-(B), (c)(1)(B) (1994)). Section 2703(b)(1) provides in pertinent part:

> A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection–
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or
>
> (ii) obtains a court order for such disclosure under subsection (d) of this section . . . .

18 U.S.C. § 2703(b)(1). Section 2703(c)(1)(B) provides:

> A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity –
>
> (i) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;
>
> (ii) obtains a court order for such disclosure under subsection (d) of this section; or
>
> (iii) has the consent of the subscriber or customer to such disclosure.

18 U.S.C. § 2703(c)(1)(B).

[30] McVeigh, 983 F. Supp. at 220 (citing Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996)). The *Tucker* court compared § 2703(a) and (b) to § 2703(c), and held that § 2703(a) and (b) are limitations on governmental conduct, in contrast to § 2703(c), which limits the conduct of service providers. *See Tucker*, 83 F.3d at 692.

11. The court, though, read § 2703(c) in conjunction with §§ 2703(a) and (b) and concluded that "all of the subsections of 2703 were intended to work in tandem to protect consumer privacy."[31] Therefore, § 2703 requires the government to obtain proper access to information stored by an ISP. The statute is a limitation on government conduct, not ISP conduct. Furthermore, even if the government prevailed in its interpretation of § 2703(c), McVeigh pled §§ 2703(a) and (b) in the alternative.[32] As such, the court granted McVeigh's preliminary injunction request and sternly noted that "[i]n these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed."[33]

12. The judge's decision confirmed McVeigh's right to online privacy and bolstered the privacy rights of anonymous cyberspace e-mailers.[34] McVeigh's lawyer, Christopher Wolf, indicated that Judge Sporkin's criticism of the Navy's activities would protect Internet users in that the electronic privacy laws "mean what they say and should be enforced" in the courts.[35] The Electronic Privacy Information Center supports this view, stating that AOL's disclosure of the information was not only a "clear violation of the ECPA," but a breach of AOL's "Terms of Service" contract.[36]

B. Beyond the ECPA – Contracting Privacy

13. The Chairman and CEO of AOL, Steve Case, acknowledged in a letter to AOL members that an employee disclosed Timothy McVeigh's identity to Navy officials in violation of company policy.[37] AOL attributed the "regretful incident" to

---

[31] McVeigh, 983 F. Supp. at 220.

[32] *See id*. (noting also that the paralegal failed to identify himself to the AOL representative and that "it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated").

[33] *Id*. The Navy has since agreed to provide McVeigh full retirement benefits and legal fees. *See* Bradley Graham, *Gay Sailor Takes Navy Retirement Settlement; AOL Also Will Pay For Privacy Violation*, WASH. POST, June 13, 1998, at A3.

[34] *See* Philip Shenon, *'Gay' Sailor's Dismissal is Blocked*, N.Y. TIMES, Jan. 27, 1998, at A8.

[35] *Id*.

[36] Bill Pietrucha, *McVeigh Still in Navy Pending Court Ruling*, NEWSBYTES NEWS NETWORK, Jan. 21, 1998, *available in* 1998 WL 5028842 (quoting David Sobel, legal counsel for the Electronic Privacy Information Center).

[37] *See* Letter from Steve Case, Chairman and C.E.O. of AOL, to AOL members (Jan. 23, 1998) (on file with the *Boston University Journal of Science & Technology* Law). The letter states, in pertinent part:

"human error,"[38] but reasserted its commitment to preserve its members' confidentiality: "It is incumbent on our industry to answer the call of consumers for greater privacy, and we believe we can do that without more legislation . . . . We are advocates for self-regulation, and we believe we can set the standard."[39] AOL apologized to McVeigh and settled with him for an undisclosed sum.[40]

14. The AOL employee's mistake was in direct contravention of AOL's Terms of Service Agreement. Under this agreement, AOL agrees not to use or disclose information about its subscribers.[41] In light of the McVeigh incident, however, AOL took additional steps to assure subscribers that AOL employees would adhere to the agreement by providing additional job training and testing for AOL's 5000 employees.[42] AOL now also requires employees to review regularly and sign its

---

> [I]t is with regret that we recently learned about an incident that compromised the privacy of one of our members, a Navy sailor. A member services representative received a call from somebody who later turned out to be a Navy investigator but called himself a friend of the member. The caller asked us to confirm that a screen name that was on something he had received was the AOL member's. Our employee should have refused to do this. Unfortunately, he did confirm the member's identity to the caller.

Id.

[38] *See id*.

[39] Mary Leonard, *Navy Drops 'Don't Ask' Case*, BOSTON GLOBE, June 13, 1998, at A3 (citing Tricia Primrose, AOL spokeswoman).

[40] *See id*. (citing Christopher Wolf, McVeigh's attorney).

[41] *See id*. In its Terms of Service Agreement, AOL agrees

> not to disclose identity information to third parties that would link a Member's screen name(s) with a Member's actual name, unless required to do so by law or legal process served on AOL, Inc. (e.g., a subpoena). AOL Inc., at its sole discretion reserves the right to make exceptions to this policy in extraordinary circumstances (such as a bomb or suicide threat, or instances of suspected illegal activity) on a case-by-case basis.

Multimedia Docket Sheet, MULTIMEDIA & WEB STRATEGIST, Jan. 1998, at 9, (citing AOL's Terms of Service Agreement); *see also* Jeremy Pomeroy, *Privacy Peril; Online Anonymity Can Be Illusory Under Current Law, ISP Policies*, MULTIMEDIA & WEB STRATEGIST, Sept. 1998, at 1 (citing AOL's "Eight Principles of Privacy").

[42] *See* Leonard, *supra* note 39.

privacy policy and will fire employees for disclosing information without authorization.[43]

15. Generally, the ECPA prohibits ISPs from disclosing the contents of stored e-mail to any person or entity unless one of its enumerated exceptions applies.[44] These exceptions range from consensual e-mail disclosures by either the sender or recipient to disclosures that the ISP may require to protect or service its

---

[43] *See* Laura Myers, *Navy Settles Dismissal Lawsuit: Sailor Will Receive Benefits*, TULSA WORLD, June 13, 1998, at 11.

[44] *See* 18 U.S.C. § 2702(a)-(b) (1994) (prohibiting disclosure of electronic communications). These subsections provide in pertinent part:

> (a) Prohibitions.—Except as provided in subsection (b)—
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
> (b) Exceptions.—A person or entity may divulge the contents of a communication—
> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
> (2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
> (6) to a law enforcement agency, if such contents—
> (A) were inadvertently obtained by the servicer provider; and
> (B) appear to pertain to the commission of a crime.

Id.

system.[45] The ECPA, however, does permit the disclosure of records pertaining to an individual's name, billing address, and length or type of service to persons other than the government.[46] The ECPA requires the government only to obtain legal process to access stored e-mail communications, records, or other information about a subscriber.[47] ISPs such as AOL may go beyond the ECPA privacy protections, however, and contractually agree to protect a subscriber's records and individual information from the general public.

16. In the future, as ISPs find their systems and privacy policies compromised by human error, subscribers may see their pricing plans altered to reflect the amount of protection offered. "No-privacy or low-privacy systems may be less expensive, while high-privacy systems may charge a premium for that service."[48] ISPs will undoubtedly pass along increased costs associated with employee training, technological improvements, and operator liability to subscribers.

III. E-MAIL IN THE WORKPLACE

17. Similar to commercial ISPs, employers must grapple with privacy concerns when operating an in-house e-mail system. In a 1996 workplace study, the ACLU estimated that employers searched the e-mail of 20 million employees.[49] A 1997 study of human resource managers found that while eighty percent of the surveyed managers used e-mail in their workplace, only thirty-six percent instituted plans addressing permissible e-mail uses, and only thirty-four percent had a written plan governing e-mail privacy.[50] Absent notification or a written waiver, employees may expect that their e-mail is private. Whether this expectation is reasonable or not may depend on how courts balance employers' rights to access stored information against employees' rights to privacy on a widely accessible system.

---

[45] *Id.*

[46] *See generally* 18 U.S.C. § 2703(a)-(c); *see also supra* note 29 and accompanying text (describing the requirements for governmental entities to obtain access to stored communications and records maintained by an ISP).

[47] *See* 18 U.S.C. § 2703(a)-(c).

[48] ROSE, *supra* note 5, at 172.

[49] *See* Rochelle Sharpe, *A Special News Report About Life on the Job — and Trends Taking Shape There*, WALL ST. J., Sept. 10, 1996, at A1.

[50] *See* Richard J. Loftus et al., *Cutting-Edge Tech Can Be Double-Edged Sword*, NAT'L L.J., Nov. 3, 1997, at B11.

18. The ECPA authorizes electronic communication service providers to access stored electronic communications.[51] An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[52] The broad language of the statute arguably applies to an employer that provides an e-mail system to its employees. In addition to access, the ECPA permits disclosure of the contents of stored electronic communications "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service."[53] ISPs and, arguably, employers may also disclose the contents of stored electronic communications for "business purposes" when they need to service a system or protect their rights or property.[54] A further exception allows ISPs and, perhaps, employers to disclose the contents of inadvertently obtained electronic communications to a law enforcement authorities if the contents "pertain to the commission of a crime."[55]

A. *Bohach v. City of Reno*

19. In one of the few reported cases interpreting the ECPA, a court held that the access exception applied to a city that provided a visual display pager system to police officers.[56] In *Bohach v. City of Reno*, police officers faced an internal affairs investigation based on the contents of stored pager messages.[57] The officers brought both Fourth Amendment and ECPA claims against the city.[58]

20. First, the court rejected the officers' constitutional claim, holding that the officers did not have a reasonable expectation of privacy in their stored communications because many people had access to the system.[59] In deciding the statutory claim, the court distinguished "intercepted" communications that are

---

[51] *See* 18 U.S.C. § 2701(c) (stating that prohibitions against accessing "a facility through which an electronic communication service is provided" do not apply to "conduct authorized by the person or entity providing a wire or electronic communication service").

[52] 18 U.S.C. § 2510(15).

[53] 18 U.S.C. § 2702(b)(3).

[54] 18 U.S.C. § 2702(b)(5).

[55] 18 U.S.C. § 2702(b)(6)

[56] *See* Bohach v. City of Reno, 932 F. Supp. 1232, 1237 (D. Nev. 1996).

[57] *See id* at 1233.

[58] *See id*. at 1234, 1235-36.

[59] *See id* at 1235.

subject to Title I of the ECPA from stored communications that are subject to Title II.[60] An "intercept" is a "contemporaneous acquisition of [a] communication through the use of [a] device."[61] Because the pager messages were already stored in the system's computer, they could not be intercepted.[62] Consequently, the court applied Title II and concluded that the access provision "allows service providers to do as they wish when it comes to accessing communications in electronic storage."[63] Thus, as a service provider, the City of Reno and its employees could not be liable under the stored communication provisions of the ECPA.[64] The court further noted that even if the "intercept" provisions of Title I applied, the court would likely find that the officers had authorized disclosure by giving prior consent to the city "in light of the plaintiffs' decision to send those messages via the computer."[65]

21. While *Bohach* applied the ECPA to a pager system and a governmental employer, *Bohach*'s reasoning suggests that neither the Constitution nor the ECPA prohibit employers from accessing and divulging the contents of employee e-mail.

B. *Smyth v. Pillsbury Co.*

22. Although the court in *Smyth v. Pillsbury Co.* referred neither to the ECPA nor to judicial definitions of interception, it similarly concluded that employers may read and divulge employee electronic communications with impunity.[66] Pillsbury installed an e-mail system to "promote internal corporate communications between its employees."[67] The company promised its employees that their e-mail was private and that its contents "could not be intercepted and

---

[60] *See id* at 1235-6.

[61] *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).

[62] *See Bohach*, 932 F. Supp. at 1236.

[63] *See id.*

[64] *See id.*

[65] *Id.* at 1237; *see also* 18 U.S.C. § 2511(2)(c) (1994) (providing that "[i]t shall not be unlawful . . . for a person acting under color of law to intercept . . . an electronic communication, where . . . one of the parties to the communication has given prior consent to such interception).

[66] *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996). Although the court stated that the employee's e-mail was "intercepted," the Pillsbury supervisor probably accessed and retrieved the subject e-mail from electronic storage. *See id.* at 98; *see also Employee Has No Privacy Right in E-Mail, District Court Rules*, COMPUTER LAW., Mar. 1996, at 24, 25 ("Pillsbury management obtained copies of the e-mail . . . .").

[67] *See Smyth*, 914 F. Supp. at 98.

used by [Pillsbury] against [them] for termination or reprimand."[68] Relying on this purported privacy, an employee sent unprofessional and derogatory messages from his home computer in response to e-mail sent by his supervisor.[69] Based on these messages, Pillsbury fired the employee, and Smyth sued for wrongful termination of his at-will employment.[70] Smyth claimed that "his termination was in violation of 'public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law.'"[71]

23. Recognizing that an invasion of privacy is a common law tort based upon an "intrusion upon seclusion," the court defined the cause of action by referencing section 652B of the Restatement of Torts.[72] Although acts such as opening someone's mail may constitute an intrusion upon seclusion,[73] only those intrusions that are "substantial and . . . highly offensive to the 'ordinary reasonable person'" create liability.[74] To determine whether the alleged invasion of privacy was substantial and highly offensive to a reasonable person, the *Smyth* court applied a balancing test similar to that used under a Fourth Amendment analysis.[75] Like the *Bohach* court, the *Smyth* court did not find that employees had a reasonable expectation of privacy in their e-mail.[76] Similarly, the court noted that the employee voluntarily communicated over the company owned e-mail system, which everyone at the company used.[77] In contrast to mandatory urine tests or personal

---

[68] *Id*.

[69] *See id*. Although Pillsbury promised e-mail privacy, the plaintiff could not establish a civil cause of action based upon the breach. *See id*. at 100 n.2. "[A]n employer may not be estopped from firing an employee based upon a promise, even when reliance is demonstrated." *Id*. (citing Paul v. Lankenau Hosp., 569 A.2d 346 (Pa. 1990)).

[70] *See id*. at 98.

[71] *Id*. at 100.

[72] *See id*. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[73] *See id*. cmt. b.

[74] *Smyth*, 914 F. Supp. at 100 (citing Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 621 (3d Cir. 1992)).

[75] *See id*.

[76] *See id*. at 101.

[77] *See id*.

property searches, Pillsbury had not required Smyth to disclose anything; instead, Smyth voluntarily used the e-mail system to communicate his opinions.[78]

24. The court also suggested that, even if Smyth had established a reasonable expectation of privacy in the e-mail, it would not find Pillsbury's interception "to be a substantial and highly offensive invasion of his privacy."[79] Pillsbury had not "requir[ed] the employee to disclose any personal information about himself or invad[ed] the employee's person or personal effects."[80] Furthermore, "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[81]

C. *Strauss v. Microsoft Corp.*

25. Although employers have succeeded against employee ECPA and invasion of privacy claims, the evidentiary nature of e-mail allows employees to use messages in court to support employment discrimination claims.[82] In the sexual discrimination case, *Strauss v. Microsoft Corp.*, an employee successfully defended a motion in limine to exclude offensive remarks and e-mail messages sent by her employer.[83] Microsoft's motion sought to exclude the following statements and e-mail:

> [Strauss's supervisor] referred to another woman in the office as the "Spandex Queen;" . . . told a temporary receptionist that he would give her $500 if she would permit him to call her "Sweet Georgia Brown;" . . . referred to himself as the "president of the Amateur Gynecology Club;" . . . forwarded to the Journal staff an e-mail advertisement for replacement "Mouse Balls;" . . . forwarded to a male Journal staff member an e-mail message containing a Reuter's news report on Finland's

---

[78] *See id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*; *see also* ROSE, *supra* note 5, at 179 (discussing a California case that held a California statute prohibiting electronic surveillance of employees did not cover e-mail).

[82] *See, e.g.*, Anthony J. Dreyer, *When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence*, 64 FORDHAM L. REV. 2285, 2297-98 (1996).

[83] *See* Strauss v. Microsoft Corp., No. 91 Civ. 5928 (SWK), 1995 WL 326492, at *5 (S.D.N.Y. June 1, 1995).

> proposal to institute a sex holiday; . . . [and] forwarded a parody of a play entitled "A Girl's Guide to Condoms" to a male staff member via e-mail who later forwarded it to [Strauss].[84]

Strauss also "received an e-mail message containing a satirical essay entitled 'Alice in UNIX Land.'"[85] Microsoft sought to exclude these e-mail messages under Federal Rules of Evidence 401, 402, and 403, claiming that they were "irrelevant, unfairly prejudicial, and would confuse and mislead the jury."[86]

26. The court did not accept Microsoft's argument.[87] In denying Microsoft's motion, the court noted that the e-mail messages were relevant as evidence of pretext.[88] Although Microsoft contended that gender discrimination did not play a role in its promotion and termination policies, the court found that the e-mail messages might lead a reasonable jury to conclude that Microsoft's stated practices were merely a pretextual cover for sexual discrimination.[89] Microsoft argued that even if the e-mail was relevant, "it should be excluded under Rule 403 because its probative value is outweighed by the danger of unfair prejudice."[90] Microsoft characterized the e-mail as "attempts at humor" and not evidence of promotion and termination decisions.[91] The court, however, found Microsoft's argument unpersuasive and stated that the evidence was probative and not prejudicial, even if "embarrassing or offensive."[92]

27. The *Microsoft* decision illustrates that e-mail represents a double-edged sword for corporate employers. As corporations reduce their employees' expectations of privacy in messages sent on company systems, employees increasingly use the unprotected communications to pursue litigation against the employer. Based on the limited number of reported decisions, corporations and employees must re-evaluate their e-mail practices. In the absence of a uniform approach to resolving privacy and discovery issues, current case law can at best

---

[84] *Id.* at *4.

[85] *Id.* at *4.

[86] *Id.*

[87] *See id.* at *4-*5.

[88] *See id.* at *4.

[89] *See id.*

[90] *Id.* at *5.

[91] *See id.*

[92] *Id.*

serve as a skeletal model for workplace policy. Employers should notify their employees that their e-mail is subject to access and future discovery in litigation. Even if employers have a written policy protecting employees' e-mail privacy, the messages are subject to discovery requests from inquiring plaintiffs who want to use the messages to prove allegations ranging from copyright and trademark infringement to sexual discrimination. Because e-mail is not "sacred," both employers and employees must take an offensive position to protect electronically stored communications. Employers should regularly delete corporate back-up files, and employees should receive notice and acknowledge in writing that they understand the ramifications of incriminating e-mail.

IV. ATTORNEY - CLIENT CONFIDENTIALITY

28. Many attorneys increasingly use the Internet to communicate with other professionals, clients, and the community. Most law firms provide Internet e-mail addresses on letterheads, business cards, and Web sites. Lexis Counsel Connect joined Martindale-Hubbell Law Directory to create an e-mail address for listed lawyers.[93] In light of the widespread use of electronic communications in the legal profession, attorneys have an ethical responsibility to consider whether their clients' confidences are adequately protected.

29. The American Bar Association Model Rules of Professional Conduct ("Model Rules") require lawyers to keep information relating to the representation of their clients confidential unless the client consents to its disclosure.[94] "The principle of confidentiality is given effect in two related bodies of law, the attorney-client privilege . . . in the law of evidence and the rule of confidentiality established in professional ethics."[95] As a rule of evidence, the attorney-client privilege protects communications and work product.[96] As a rule of confidentiality, Model Rule 1.6 extends the privilege beyond attorney-client communications to encompass any information connected to the representation.[97] To ensure that client confidences are maintained in cyberspace, attorneys have an ethical responsibility to take

---

[93] *See* William P. Matthews, Comment, *Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 U. KAN. L. REV. 273, 295 (1996).

[94] *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6(a) (1998) ("A lawyer shall not reveal information relating to the representation of a client unless the client consents after consultation, except for disclosures that are implicitly authorized in order to carry out the representation . . . .").

[95] *Id*. cmt. 5.

[96] *See id*.

[97] *See id*.

reasonable steps toward safeguarding e-mail communications that may have an adverse impact on their clients' cases.[98]

30. A number of state bar organizations have written advisory opinions to guide attorneys through the muddy waters created by the lack of case law concerning e-mail confidentiality.[99] Although the opinions all invoke Model Rule 1.6, some are contradictory.[100] While some of the opinions reflect technological considerations, the ethics boards "have displayed an imperfect or incomplete understanding of existing technology."[101] Several of the opinions compare e-mail to telephone and fax communications.[102] Relying on the intercept provisions of the ECPA, the Illinois State Bar Association concluded that "the expectation of privacy for electronic mail is no less reasonable than the expectation of privacy for ordinary telephone calls . . . ."[103] Title I of the ECPA expressly preserves the privileged nature of illegally intercepted e-mail.[104] Therefore, an attorney will not violate Model Rule 1.6 by communicating with a client via e-mail, and unauthorized e-mail interceptions will not destroy the attorney-client privilege.

31. When the state bar associations compare e-mail to telephone conversations and focus on Title I's "intercept" provisions, however, they ignore that most e-mail is stored.[105] As such, Title II of the ECPA, pertaining to electronic storage, applies. Although *intercepted* e-mail retains its privileged character under Title I, Title II does not have a corresponding provision for *stored* communications.

---

[98] *See generally* Wendy R. Leibowitz, *'Can We Talk?' E-Mail Is Ethics Maze*, NAT'L L.J., Aug. 18, 1997, at A1, A11. *Cf. Attorneys–Confidentiality: ABA Panel Allows Unencrypted E-Mail for Transmitting Confidential Information*, 67 U.S.L.W. 2645 (May 4, 1999) (stating that attorneys may use "all forms" of e-mail without obtaining client consent because "[e]-mail communications pose no greater risk of interception and disclosure than other modes of communication that lawyers commonly use and expect to be private").

[99] *See id*. at A1.

[100] *Id*.

[101] *Id*. (citing Peter Krakaur, "a San Francisco attorney who is president of Internet Legal Services, a company that hosts a Web site dedicated to legal ethics.").

[102] *See* Alaska Bar Ass'n Ethics Comm., Ethics Op. 98-2 (1998), *available in* 1998 WL 156443; S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997), *available in* 1997 WL 582912; Ill. Bar Ass'n, Advisory Op. on Professional Conduct 96-10 (1997), *available in* 1997 WL 317367.

[103] Ill. Bar Ass'n, Op. 96-10 (1997), *available in* 1997 WL 317367, at *4.

[104] *See id*. (citing 18 U.S.C. § 2517(4) (1996) ("No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."); *see also* Alaska Bar Ass'n Ethics Comm., Ethics Op. 98-2 (1998), *available in* 1998 WL 156443, at *1 (citing to § 2517(4) also).

[105] *See generally* Bert L. Slonim, *E-Mail and Privileged Communications*, N.Y. L.J., Nov. 17, 1997, at S3, S13.

Additionally, attorneys may be misled by bar association opinions that refer to *intercepted* e-mail, but cite Title II prohibitions against unauthorized access and disclosure of *stored* communications.[106] Although such access and disclosure is illegal under Title II, Title II does not address the issue of privileged communications and information. Nonetheless, in the absence of statutory protection, Model Rule 1.6 imposes an ethical duty on lawyers to use "reasonable measures," interpreted to mean "ordinary, everyday measures," to protect client confidences.[107]

32. The Pennsylvania Bar Association advises lawyers that they "may use e-mail to communicate with or about a client without encryption."[108] The lawyer, however, should consult with the client and advise him of the risks of using e-mail.[109] The lawyer should also obtain the client's consent to use e-mail, especially in cases where intercepted, unencrypted e-mail might damage the client's case.[110] Additionally, the Association advises that lawyers "place a notice on client e-mail warning that it is a privileged and confidential communication . . . ."[111]

33. Unlike the Pennsylvania Bar, the Iowa Bar Association encourages its attorneys to encrypt e-mail unless the client "consents to unencrypted

---

[106] *See* S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997), *available in* 1997 WL 582912, at *2 ("[B]ecause the interception of e-mail is now illegal under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701(a) and 2702(a), use of e-mail is proper under Rule 1.6."). Although the South Carolina Bar uses the term "intercept," § 2701(a)(1) and (2) make it unlawful to *access* stored communications without authorization, and § 2702(a) prohibits the disclosure of contents of a communication in electronic storage. *See* 18 U.S.C. §§ 2701(a)(1)-(2), 2702(a) (1998).

[107] *See* Pa. Bar Ass'n Comm. on Legal Ethics & Prof. Resp., Informal Op. 97-130 (1997), *available in* 1997 WL 816711, at *2.

[108] *Id*. at *5; *see also* Alaska Bar Ass'n Ethics Comm., Ethics Op. 98-2 (1998), *available in* 1998 WL 156443, at *2 n.2 ("Encrypted e-mail has been electronically locked to prevent anyone but the intended recipient from reading it, using a 'lock and key' technology. Simply stated, such messages are 'locked' by the sender, making them unreadable except by the intended recipient, who has a 'key' in the form of an electronic password to decode the message.").

[109] *See* Pa. Bar Ass'n Comm. on Legal Ethics & Prof. Resp., Informal Op. 97-130 (1997), *available in* 1997 WL 816711, at *5.

[110] *See id*. at *6. *But see Attorneys–Confidentiality*, *supra* note 98, at 2645 (reporting on ABA panel's decision that attorneys need not obtain prior client consent before using e-mail).

[111] *Id*.; *see also* N.C. St. Bar, Ethics Op. RPC 215 (1995), *available in* 1995 WL 853887, at *1 ("First, the lawyer must use reasonable care to select a mode of communication that, in light of the exigencies of the existing circumstances, will best maintain any confidential information that might be conveyed in the communication. Second, if the lawyer knows or has reason to believe that the communication is over a telecommunication device that is susceptible to interception, the lawyer must advise the other parties to the communication of the risks of interception and the potential for confidentiality to be lost.").

communication."[112] South Carolina advises "that a finding of confidentiality and privilege of such communications [under the ECPA does] not end the analysis."[113] To fulfill their duty to use reasonable care in keeping client communications confidential, lawyers should "discuss with [clients] such options as encryption."[114] The Alaska Bar notes that "[g]iven the increasing availability of reasonably priced encryption software, attorneys are encouraged to use such safeguards when communicating particularly sensitive or confidential matters by e-mail, i.e., a communication that the attorney would hesitate to communicate by phone or by fax."[115] Recent commentators lend support to the Alaska opinion by citing the sage advice of Judge Learned Hand in *The T.J. Hooper* case.[116] In that case, tugboat operators lost cargo at sea because their boat did not have a radio, which would have provided advance warning of the impending storm.[117] Judge Hand found the tugboat owners liable because other shippers used the technology.[118] Thus, in light of the low cost and ease of installation, attorneys should use encryption software to protect e-mail communications relating to their clients' representation.

V. CONGRESSIONAL AND INDUSTRIAL DEVELOPMENTS

34. In addition to e-mail's susceptibility to unauthorized access and disclosure, private and public entities further marginalize individual privacy by maintaining vast data bases of stored information pertaining to people's credit history, medical records, and purchasing habits. Third parties can access, disclose,

---

[112] Slonim, *supra* note 105 (citing Iowa Bar Ass'n, Formal Op. 96-1 (1996)). *Cf.* Pa. Bar Ass'n Comm. on Legal Ethics & Prof. Resp., Informal Op. 97-130 (1997), *available in* 1997 WL 816711, at *5.

[113] S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997), *available in* 1997 WL 582912, at *3.

[114] *Id.*

[115] Alaska Bar Ass'n Ethics Comm., Ethics Op. 98-2 (1998), *available in* 1998 WL 156443, at *1.

[116] The T.J. Hooper v. Northern Barge Corp., 60 F.2d 737 (2d Cir. 1932); *see also* Leibowitz, *supra* note 98, at A11. *See generally* Stephen Masciocchi, *Internet E-Mail: Attorney-Client Privilege, Confidentiality, and Malpractice Risks*, COLO. LAW., Feb. 1998, at 61, 63 (1998).

[117] *See The T.J. Hooper*, 60 F.2d at 737.

[118] *See id.* at 740 ("[W]hen some have thought a device necessary, at least we may say that they were right, and the others too slack."); *see also* Leibowitz, *supra* note 98, at A11 (stating that future judges could possibly consider a lawyer's failure to use encryption programs when sending confidential information over e-mail as a negligent breach of the attorney-client privilege).

and market these records without the sources' knowledge or permission.[119] The Commerce Department reported that an estimated 62 million Americans used the Internet, and approximately "10 million people across the United States and Canada made purchases–from airline tickets to books to automobiles–on the Web by the end of 1997, up from 7.4 million people six months earlier."[120] To address consumer concerns about online privacy, there are "some 80 different patchwork bills pending in Congress aimed at restricting the flow of intimate personal data in cyberspace, now available to anyone browsing through the World Wide Web."[121]

35. To hinder the flow of government-disclosed data, Representative Barrett introduced the Federal Internet Privacy Protection Act of 1997 ("Internet Privacy Act") in the House of Representatives.[122] This Act would have prohibited federal agencies from making an individual's confidential records available on the Internet.[123] It defined a "record" as

> any item, collection, or grouping of information about an individual that–
>
> (1) is maintained by an agency with respect to the education, financial transactions, medical history, or employment history of the individual; and
>
> (2) contains the name or the identifying number, symbol, or other identifying particular assigned to the individual.[124]

An individual who "suffer[ed] harm" through the release of information on the Internet, either before or after passage of the Internet Privacy Act, "may bring a civil action against the agency."[125]

36. In addition, Representative Vento introduced legislation in the House aimed at protecting subscriber information from unauthorized disclosure by

---

[119] *See* 18 U.S.C. § 2703(c)(1)(A) (1994) ("[A] provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service . . . to any person other than a governmental entity.").

[120] Ted Bridis, *Purchases Powering the Internet*, CHI. SUN-TIMES, Apr. 16, 1998, at 3.

[121] Peter Maas, *How Private Is Your Life?*, BOSTON GLOBE, Apr. 19, 1998, (Parade Magazine) at 4.

[122] *See* H.R. 1367, 105th Cong. (1997).

[123] *See id*.

[124] *Id*. § 2(c).

[125] *Id*. § 2(b).

interactive computer service providers.[126] The Consumer Internet Privacy Protection Act ("Consumer Privacy Act") would have required providers to obtain an individual's written revocable consent prior to disclosing "any personally identifiable information."[127] Even if a subscriber consented, he had the right to verify the contents of stored records, correct any errors, and request that the provider identify third parties seeking the information.[128] Providers could not charge subscribers a fee for services rendered under the Consumer Privacy Act.[129] To enforce the Act's provisions, the Federal Trade Commission would have monitored providers and issued cease and desist orders for discovered violations of the Act.[130] Additionally, the Act provided a private civil cause of action for subscribers harmed by wrongful disclosures.[131]

37. An amendment to Title 15 curtailed the unauthorized collection of information about children.[132] The Children's Online Privacy Protection Act of 1998 ("Children's Act") makes it unlawful for "an operator of a website or online service directed to children . . . to collect personal information from a child in a manner that violates the [act's] regulations."[133] The amendment is aimed at Web sites or online services "directed to children that collects personal information from children."[134] The Children's Act requires that these sites or services contain a notice that the sites collect information and explain the sites' uses and disclosure practices with the information.[135] Upon parental request, the Children's Act

---

[126] *See* H.R. 98, 105th Cong. (1997). The Social Security On-line Privacy Protection Act of 1997 is narrower in scope, but similar to the Consumer Internet Privacy Act. *See* H.R. 1287, 105th Cong. (1997). The bill prohibits interactive computer service providers from disclosing social security numbers or similar personal information without the subscriber's consent. *See id*. § 2(a).

[127] H.R. 98, 105th Cong. § 2(a) (1997).

[128] *See id*. § 2(c).

[129] *See id*. § 2(c)(3).

[130] *See id*. § 3(a)-(b).

[131] *See id*. § 3(b)(2).

[132] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as amended at 15 U.S.C. §§ 6501-06 (1999)).

[133] 15 U.S.C. § 6502(a)(1) (1999).

[134] *See id*. § 6502(b)(1)(A).

[135] *See id*. *See also Consumer Protection–Privacy: FTC Child Privacy Protection Proposal Mandates Verifiable Parental Consent*, 67 U.S.L.W. 2631 (Apr. 27, 1999) (reporting on the Federal Trade Commission's proposed rule for enforcing the Children's Act, which delegated enforcement to the Commission).

requires a site to disclose the information collected and cease from using or maintaining the collected information.[136]

38. While the United States debates privacy laws, other countries have adopted privacy policies. Because the Internet is a global conglomerate of networks, differing privacy approaches are bound to create international discord. The European Union Data Protection Directive ("European Directive") would apply when an individual processes personal data manually or automatically with a computer.[137] Like current and proposed American legislation, the European Directive authorizes the processing of personal data if the processor notifies the subject individual and receives consent to disseminate the information.[138] Subject individuals must freely consent and have knowledge of how the data is to be used, accessed, and disclosed.[139]

39. The European Directive carves out several exceptions to the consent requirement. For example, data processing undertaken to maintain the law and keep public order, to perform a contract, or protect the interests of service providers may be performed without prior consent.[140] "These interests have to be weighed against those of the data subject," however.[141] Thus, in the case of third party disclosures, an individual has the right to know who wants the information and the right to erase the information without having to pay a service charge.[142] The European Directive grants the agency responsible for implementing the regulation investigative and enforcement powers and also provides civil remedies for violations of data privacy.[143]

40. Initially, the European privacy policy "prohibited the transfer of data to . . . countries which did not provide for an 'adequate' level of protection."[144] If the term "adequate" were interpreted as "equivalent," countries like the United States

---

[136] *See* 15 U.S.C. § 6502(b)(1)(B).

[137] *See* Peter Menyasz, *U.S. Move to Privacy Legislation Seen as 'Inevitable' Over Long Term*, 66 U.S.L.W. 2238, 2238 (Oct. 21, 1997) (quoting Professor Joel Reidenberg, Fordham University Law School); *see also* Ian Lloyd, *An Outline of the European Data Protection Directive*, J. INFO. L. & TECH. 1996 (Jan. 31, 1996) <http://www.elj.warwick.ac.uk/elj/jilt/dp/intros/>.

[138] *See* Lloyd, *supra* note 137.

[139] *See id.*

[140] *See id.*

[141] *Id.*

[142] *See id.*

[143] *See id.*

[144] *Id.*

would be cut out of the global stream of information transfers because they use "a sectoral approach to the problems of data processing rather than the omnibus model adopted within Europe."[145] In the amended version of the European Directive, a country's privacy policy will be deemed adequate in light of "all the circumstances surrounding a data transfer operation."[146] Attention will focus on "the nature of the data, the purpose or purposes and duration of the proposed processing operation . . . the legislative provisions, both general and sectoral, in force in the third country in question and the professional rules which are complied with in that country."[147] When a country's privacy policies are deemed inadequate, the European Directive provides alternative ways for member states to protect individuals, such as through contractual agreement based on terms provided by the International Chamber of Commerce and Council of Europe.[148]

41. The European Directive has spurred American organizations to develop their own privacy policies to meet European standards and continue to be able to conduct business within European.[149] Without data privacy protection, consumers may be reluctant to do business on the Internet.[150] To meet privacy requirements for commercial transactions, American organizations formed coalitions to address the European Directive challenges. For example, the Information Technology Industry Council ("ITI") established voluntary guidelines to promote online privacy and electronic commerce.[151] Entitled "The Protection of Personal Data in Electronic Commerce," the ITI's platform applies "not only to data collection practices on the Internet but also to ITI members' use of electronic databases."[152] ITI developed the guidelines using a "sectoral approach" to permit flexibility within the industry while promoting a variety of privacy options for consumers.[153] The council contends

---

[145] *Id.* A "sectoral" approach seems to indicate privacy reform based on self-regulatory commercial policies that are adaptable to a broad spectrum of industries, as opposed to piecemeal statutory regulation directed towards solving specific problems within a particular industry. *See Technology Trade Group Offers Information Age Privacy Guidelines*, 66 U.S.L.W. 2399, 2399 (Jan. 6, 1998).

[146] Lloyd, *supra* note 137.

[147] *Id.*

[148] *See id.*

[149] *See* Menyasz, *supra* note 137, at 2238.

[150] *See id.*

[151] *See Technology Trade Group Offers Information Age Privacy Guidelines*, *supra* note 145, at 2399. ITI's Web site address is <http://www.itic.gov/>.

[152] *Id.* (quoting Christopher Hankin, director of government affairs for the cash register manufacturer, NCR).

[153] *See id.*

that a "one-size-fits-all approach would result in limited individual choice, prevent maximum participation in electronic commerce, and b[e] overly cumbersome and costly."[154]

42. The ITI guidelines contain eight principles:

> (1) Companies' data collection policies should be disclosed and easily understood.
>
> (2) Individuals have the right to make informed decisions about the use of their personal data. Technological solutions that empower individuals to exercise control over their personal data can often provide greater personal data protection.
>
> (3) Data collection should be limited to valid business purposes and should be obtained legally and fairly.
>
> (4) Collected information should be kept accurately and individuals should have the opportunity to review and correct personal data in a defined and secure manner.
>
> (5) Individuals should be informed about the use of personal data collected and have the ability to direct that the information not be disclosed.
>
> (6) Steps should be taken to ensure that collected data is not subject to unauthorized access and disclosure.
>
> (7) Consumer awareness respecting the importance of fair information practices and privacy protection should be fostered, and individuals should use their marketplace powers to protect their personal data and that of their children.
>
> (8) To the extent possible, privacy principles and practices should be the same irrespective of the technology employed for its collection and use. Individuals should have reasonably consistent privacy expectations whether they are operating in an electronic or paper-based environment.[155]

ITI anticipates that these guidelines will satisfy the Clinton Administration's challenge to industry "to develop self-regulatory solutions to the privacy challenges posed by sweeping technology advances that greatly facilitate the collection, compilation, and distribution of personal information."[156]

---

[154] *Id.*

[155] *Id.*

[156] *Id.*

43. The Individual Reference Services Group ("IRSG"), a "consortium of look up services providers," received the FTC's approval of its privacy guidelines for disseminating personal information.[157] In light of the IRSG's plan, the FTC's chairman stated he would not recommend congressional legislation addressing the illegal use of personal data assuming the plan would reduce identity fraud.[158] Under the plan, members of the IRSG agree not to disseminate social security numbers that they gather from non-public sources on the Internet.[159] The guidelines require that members allow consumers to access their personal information "opt out" of its dissemination.[160] Additionally, members agree that personal information about minors will not be disseminated "to the general public or to commercial and professional companies."[161]

44. Although many industry coalitions are implementing policies to increase protection of personal information, it is not clear that private self-regulation satisfies the European Directive.[162] One source of direction behind the European Directive clearly preferred the enactment of U.S. legislation over self-regulation to provide adequate protection.[163] An official of the European Directive's U.S. delegation, however, stated that "strong privacy protections in the financial services sector, industry-led codes of conduct, and public sentiment in favor of some form of federal privacy entity" demonstrated a positive degree of compliance with European Directive goals.[164]

---

[157] *See FTC Backs Industry Plan for Self-Regulation on Dissemination of Sensitive Personal Data*, 66 U.S.L.W. 2389, 2389 (Jan. 6, 1998).

[158] *See id.*

[159] *See id.* at 2390; *see also* Ted Bridis, *Retail Trade Group Announces Privacy Guidelines*, Associated Press Pol. Serv. (Apr. 15, 1998), *available in* 1998 WL 7405122. The National Retail Federation issued voluntary guidelines for consumer privacy after Independent Counsel Kenneth Starr subpoenaed two Washington, D.C. bookstores' credit card receipts for information on Monica Lewinsky's purchases. *See id.*

[160] *See id.*

[161] *Id.*

[162] *See FTC Backs Industry Plan for Self-Regulation on Dissemination of Sensitive Personal Data*, *supra* note 157, at 2389.

[163] *See id.* The Department of Commerce has issued International Safe Harbor Privacy Principles that deem qualifying organizations as providing "adequate protection of personal data." Nadya Aswad, *Telecommunications–Internet Privacy: Commerce Revises Safe Harbor Principles, Answers Frequent Questions on Data Access*, 67 U.S.L.W. 2636 (Apr. 27, 1999).

[164] *See FTC Backs Industry Plan for Self-Regulation on Dissemination of Sensitive Personal Data*, *supra* note 157, at 2390 (quoting John B. Richardson, deputy head of the European Commission's Washington delegation) ("The EU will not expect the United States to comply 'one hundred percent'

45. The Center for Democracy & Technology ("CDT") is an organization dedicated to "practical solutions to enhance free expression and privacy in global communications technologies."[165] The CDT supports development and use of the Platform for Privacy Preferences ("P3P") as a foundation for privacy protection on the Internet.[166] "[P3P] allows Net surfers and content providers to agree on the standards for use of personal information."[167] The P3P standard allows Web sites to "express their privacy practices" and Web site visitors to "exercise preferences over those practices."[168] With P3P, users can configure their privacy preferences and "seamlessly" access those sites that match their preferences.[169] When attempting to access Web sites with noncomplying privacy practices, the P3P system notifies users of the sites' practices and allows the users to choose to continue to explore the sites.[170] If adopted on a universal basis, consumers will regain control of the privacy equation through the selective filtering of sites inconsistent with their data collection objectives.

VI. CONCLUSIONS

46. This Article has explored Internet privacy in a number of different scenarios. The one common thread throughout these scenarios is the need for consistent policy. Internet users have a right to expect a certain modicum of privacy in their e-mail and commercial transactions. Service providers, employers, professionals, and commercial enterprises must develop and publish their privacy policies and users can no longer rely on piecemeal legislation that lacks adaptability. The Internet is an evolving medium; a statute designed to protect e-mail privacy will not protect information about credit card purchases.

47. Besides relying on broad regulations, Internet users must develop their own personal privacy policies. Users should demand and use encryption software for sensitive communications and electronic transactions. Individuals can shape the future of the Internet by refusing to transact business with companies or visit Web sites that collect data without providing a right to access, verify, and correct

---

with the privacy standards set out in the directive; rather, we are looking for a good level of overall compliance.").

165 *See* Center for Democracy & Technology, *Our Mission*, (last visited May 7, 1999) <http://www.cdt.org/mission.shtml>.

166 *See* CENTER FOR DEMOCRACY & TECHNOLOGY, DEMOCRATIC VALUES FOR THE DIGITAL AGE (1998).

167 *Id.*

168 World Wide Web Consortium, *Platform for Privacy Preferences P3P Project* (last modified May 7, 1999) <http://www.w3.org/P3P/>.

169 *See id.*

170 *See id.*

personal information. Through vigilance and caution, users can insure that the Internet remains a valuable and safe resource.