Volume 42 | Issue 3 Article 6

1997

# E-mail in the Workplace and the Right of Privacy

Kevin J. Baum

# Comment

## E-MAIL IN THE WORKPLACE AND THE RIGHT OF PRIVACY

### I. INTRODUCTION

The foundation for the modern right of privacy traces its origins to the influential *Harvard Law Review* article coauthored by Samuel D. Warren and Louis D. Brandeis in 1890.[1] These authors proclaimed: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right 'to be let alone.'"[2] Warren and Brandeis realized that society was in a perpetual state of advancement; consequently, the American legal system also had to evolve perpetually to protect the individual's privacy rights.[3] At the turn of the century, however, the article was met with mixed reaction. Numerous courts rejected the right to privacy because past American courts had never recognized such a right.[4] Conversely, a minority of courts embraced the right to privacy thesis set forth in the article.[5] Currently, the right of privacy is firmly entrenched within the American legal system.[6]

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Professor Richard C. Turkington commented on the legal significance of the Warren and Brandeis article:

> It is likely that the Warren and Brandeis article has had as much impact on the development of law as any single publication in legal periodicals. It is certainly one of the most commented upon and cited publications in the history of our legal system. A more influential piece of scholarship is difficult to imagine. . . . The official theory of the legal right of privacy as expressed in numerous publications springs the right *eo instanti* from the pen of Warren and Brandeis in 1890.

RICHARD C. TURKINGTON ET AL., PRIVACY: CASES AND MATERIALS 31 (1992).

2. Warren & Brandeis, *supra* note 1, at 195.

3. *See id.* Warren and Brandeis authored their article in response to the mass media's "overstepping in every direction the obvious bounds of propriety and of decency." *Id.* at 196. The technology of the 1890s that Warren and Brandeis felt presented a danger to privacy interests included "[i]nstantaneous photographs and newspaper enterprise [that] have invaded the sacred precincts of private and domestic life; and numerous mechanical devices [that] threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" *Id.* at 195.

4. *See* Roberson v. Rochester Folding Box Co., 64 N.E. 442, 443 (N.Y. 1902) (rejecting right to privacy because not historically based and deferring to legislature's power to create right to privacy).

5. *See* Pavesich v. New England Ins., Co., 50 S.E. 68, 72 (Ga. 1905) ("A right to privacy in matters purely private is . . . derived from natural law.").

6. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (recognizing constitutional right to privacy). In *Griswold*, the Court recognized that a right to privacy exists under the U.S. Constitution even though the right to privacy is not expressly mentioned in the Constitution. *See id.* at 484. Justice Douglas, writing for the ma-

In today's ever increasing computerized world, the potential danger to individual privacy interests exists at a level never before seen.[7] The workplace presents a unique arena for privacy analysis. Two competing interests exist in the employment context: the employer's right to conduct business in a self-determined manner is matched against the employee's privacy interests or the right to be let alone.[8]

This Comment analyzes an employee's privacy interests relating to electronic mail ("e-mail") in the workplace. Part II discusses the basic issues that exist when an employer decides to install and maintain an e-mail system in the workplace.[9] Part III discusses the sources of law for privacy rights in the employment context: the United States Constitution, individual state constitutions, the common law and federal statutory enactments.[10] Part IV discusses two recent federal district court cases and one state court case involving e-mail privacy in the workplace.[11] Part V discusses e-mail employment policies as a possible method to alleviate the privacy concerns of both employers and employees.[12] In addition, Part V provides segments of a sample e-mail employment policy covering the ma-

---

jority, stated that specific guarantees within the Bill of Rights have penumbras "formed by emanations from those guarantees that help give them life and substance." *Id.* The guarantees within the Bill of Rights that create a constitutional zone of privacy are the First Amendment's right of association, the Third Amendment's prohibition against the quartering of soldiers, the Fourth Amendment's right against unreasonable searches and seizures, the Fifth Amendment's right against self-incrimination and the Ninth Amendment's retention of rights not specifically enumerated within the Constitution. *See id.* The Court concluded that "the right of privacy which presses for recognition [in this case] is a legitimate one." *Id.* at 485. For a further discussion of the impact of Warren and Brandeis on privacy law in the United States, see Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703 (1990); Robert C. Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 CASE W. RES. L. REV. 647 (1991).

7. *See* EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW: YOUR RIGHTS AND DUTIES IN THE ON-LINE WORLD 14 (1994) (noting immense increase in e-mail use over last three years); Ken Wasch, *Encouraging E-mail, Limiting Liability*, BUS. TIMES, Dec. 16, 1996, at 13 ("E-mail is changing the workplace in a way we have not seen since the proliferation of the telephone a century ago."); *see also* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (S.D. Ohio 1997) (discussing recent issue of commercial enterprises distributing unsolicited e-mail advertising to subscribers). For a general discussion of invasion of privacy and the private sector workplace, see John D. Blackburn et al., *Invasion of Privacy: Refocusing the Tort in Private Sector Employment*, 6 DEPAUL BUS. L.J. 41 (1993).

8. *See* Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1257 (1994) (stating that employers see monitoring as "an unrestricted prerogative of management while labor views it as a step towards an Orwellian workplace").

9. For a further discussion of the basic issues presented by e-mail in the workplace, see *infra* notes 15-34 and accompanying text.

10. For a further discussion of the sources of privacy protection, see *infra* notes 35-93 and accompanying text.

11. For a further discussion of recent case law involving e-mail in the workplace, see *infra* notes 94-120 and accompanying text.

12. For a further discussion of e-mail employment policies as a method to

jor areas of concern for e-mail privacy in the workplace.[13] Part VI concludes that, under current federal and state law, an employee has limited privacy rights for workplace e-mail and that e-mail monitoring policies should be instituted in all workplaces utilizing an e-mail system.[14]

## II. ISSUES REGARDING E-MAIL IN THE WORKPLACE

Approximately twenty million employees have access to e-mail systems in their workplaces.[15] Because of the need for advanced communications in the business world, this figure is expected to double by the year 2000.[16] E-mail communication provides employers and employees with a technological advantage in the modern workplace.[17] Along with its many benefits, employers have started to realize that the use of e-mail technology may also have complicated drawbacks.[18]

---

prevent privacy conflicts between employers and employees, see *infra* notes 121-48 and accompanying text.

13. For an example of a sample e-mail employment policy, see *infra* notes 137-41 and accompanying text.

14. For a further discussion of the conclusion of this Comment, see *infra* notes 149-58 and accompanying text.

15. *See* Lisa Donovan, *E-mail, Privacy Don't Mix: Employees Mistaken to Assume Protection*, CINCINNATI ENQUIRER, Sept. 14, 1996, at B5. This figure represents approximately one-sixth of the total work force in the United States. *See* Karen Brune Mathis, *Eyes on Your E-Mail; Messages Workers Send on Company Computers Are Often Monitored*, FLA. TIMES-UNION, July 15, 1996, at 10. Ninety percent of companies with greater than 1000 employees utilize e-mail systems. *See id.* In addition, greater than 50% of company e-mail systems have originated since 1990. *See id.* One large American company estimates that its employees transmit greater than one million e-mail messages across company networks every day. *See* Bonnie C. Glassberg et al., *Electronic Communication: An Ounce of Policy is Worth a Pound of Cure; Electronic Mail*, BUS. HORIZONS, July 1996, at 74 (discussing DuPont's use of e-mail systems).

16. *See* Holland & Hart, *E-mail and Voice Mail: Liability Waiting to Happen?*, IDAHO EMPLOYMENT L. LETTER, July 1996, at 1. According to Frank Morris Jr., a Washington, D.C. attorney, in the year 2000, the estimated forty million workplace e-mail users will generate sixty billion e-mail messages a year. *See* Mathis, *supra* note 15, at 10. In addition, a Massachusetts-based research company has estimated that e-mail use in the United States will increase from 15% to 50% of the total population by the year 2002. *See* Vanessa Houlder, *Failing to Get the Message: E-mail's Advantages Could Be Lost By Staff Misusing It*, FIN. TIMES (London), Mar. 17, 1997, at 14.

17. *See* Holland & Hart, *supra* note 16, at 1. E-mail allows employees and employers to communicate in a more efficient manner, thus saving both time and money. *See id.* In a very brief period of time, an e-mail user can communicate with another individual anywhere in the world. *See id.* In addition, an employer's clients often demand and prefer services that involve e-mail technology. *See id.*; *see also* Mark Calvey, *Electronic Communications Giving Companies a Shock*, S.F. BUS. TIMES, Aug. 2, 1996, at A11 ("[C]ompanies want employees to harness the ability of e-mail to keep in touch with colleagues, customers and suppliers day or night around the world. They are also attracted by the awesome informational capabilities of the Internet."); Donovan, *supra* note 15, at B5 (stating that e-mail is "[m]eant to increase on-the-job productivity").

18. *See* Beth Mattson, *E-mail Messages Carry Legal Pitfalls*, BUS. DATELINE, Dec.

First, e-mail communications can be discoverable evidence during a civil or criminal proceeding against an employer.[19] E-mail communica-

20, 1996, at 16 ("[A]s e-mail becomes more prevalent in today's workplace, so do the problems that result from the misuse and abuse of this communication medium."). Unlike paper, e-mail can be copied and communicated to others with much greater ease. *See* Michael Overly, *Avoid the Legal Pitfalls of E-mail*, LAN MAG., Jan. 1997, at 75 ("With the click of a mouse, an employee can send e-mail to every computer user in a company or post the e-mail on the Internet where thousands, if not hundreds of thousands, of people can read it."). One group of commentators created a list of the differences between e-mail and traditional communications medium. *See* Glassberg et al., *supra* note 15, at 74 fig.1. The list includes the following differences: "[v]erbal and visual cues are filtered out and references to status or position are lacking," "[c]opies of messages look the same as the originals," "[t]he store-and-forward system results in one or more copies being stored as backups," "[d]eleting your copy does not mean all copies are destroyed," "[m]essages, once opened, cannot be retrieved, and can be edited and forwarded without the original sender's knowledge or consent" and "[m]essages are not protected in the same way as letters; they are considered the property of the owner of the network, usually the employer." *Id.*

In addition to e-mail-specific issues, employers are also worried about employees using the Internet for personal use during work hours. Recently, software manufacturers created software programs that make it easy for an employer "to monitor every Internet transaction made from [the employee's] computer." *Is the Boss Watching You Surf the Web?*, DES MOINES REG., May 21, 1996, at 3.

19. *See* Ellen Forman, *That Office E-mail You Deleted Could End Up in Court*, SUN-SENTINEL (Fort Lauderdale), Mar. 25, 1997, at 1A ("[I]f you're an employer, E-mail can be subpoenaed by a plaintiff's lawyer and dragged out of the computer in case of a lawsuit."); Mathis, *supra* note 15, at 10 ("[E]-mail creates a permanent record of what's said, providing evidence in criminal and civil suits. The 'delete' key doesn't erase the message from back-up files."); Mattson, *supra* note 18, at 16 ("'People don't understand the permanency or potential permanency in e-mail . . . .' Deleted messages may disappear from the monitor, but until the computer writes over the space on the hard drive, the message can still be resurrected" (quoting Paul Hattouni, manager of consulting services agency)); *see also* Glassberg et al., *supra* note 15, at 74 ("Employers . . . have been asked by the courts to deliver potentially damaging evidence from corporate archives. The content of E-mail messages might potentially be used by either party in a lawsuit. So there can be serious legal consequences for the firm in simply storing messages on a long-term basis."); Mattson, *supra* note 18, at 16 (discussing court order requiring company to search through thirty million discarded e-mail messages for evidence of disputed contract, at cost of $50,000). Furthermore, e-mail presents three significant problems for a company defending a lawsuit: first, e-mail is easier to alter than a handwritten document; second, requests for e-mail production can be "onerous"; and third, e-mail messages may be inadvertently preserved for numerous years. *See* Patrick Mitchell, *Following the E-mail Trail*, COMPUTER SHOPPER, Apr. 1997, at 92.

E-mail messages are both troublesome and damaging in litigation because they are a "hybrid written memo and telephone conversation." Mathis, *supra* note 15, at 13. Employees often spend little time drafting or revising e-mail messages, as evidenced by their tendency to be "short, punchy, poorly punctuated—and potentially harmful." *Id.*; *see also* Houlder, *supra* note 16, at 14 (stating that survey of 259 United Kingdom organizations found "widespread carelessness in the way that e-mails were structured and distributed"). Attorneys refer to such uncensored e-mail messages as being "'hot documents' because such potentially incriminating statements can provide an opening to possible liability and litigation." L.A. Lorek, *E-mail Can Get the Employer in Trouble*, SUN-SENTINEL (Fort Lauderdale), Jan. 12, 1997, at G4. For further examples of litigation involving e-mail communications in the

tions are subject to the same discovery standards as paper-based communications, such as letters or memoranda.[20] In addition to being discoverable evidence, the contents of workplace e-mail may be the primary reason an employer is being sued.[21] For example, in the first reported case in which e-mail was the basis for an employment discrimination claim, two employees filed a racial discrimination lawsuit against their employer, Morgan Stanley, for sixty-million dollars after they received racially offensive material via e-mail from coworkers.[22] Although Morgan Stanley took what it termed "swift and stern action" after learning of the incident, the two employees sought recovery because the messages created a "hostile work environment," causing them to experience severe emotional and physical distress.[23] Similarly, employees of Citibank recently filed a suit in the

---

workplace, see Geanne Rosenberg, *Electronic Discovery Proves an Effective Legal Weapon*, N.Y. TIMES, Mar. 31, 1997, at D5.

E-mail communications are becoming a particular concern in the health services industry. *See* Jeffrey A. Van Doren, *If You Monitor E-mail, Have a Policy*, HEALTH CARE SUPERVISOR, Sept. 1996, at 12 ("Use of electronic mail . . . in health care institutions is a new cause for concern in monitoring confidentiality."). If an employee transmits an e-mail message violating the employer's patient confidentiality policy, the employer could be held liable and "the e-mail communication could be the proverbial smoking gun." *Id.* In addition, the use of e-mail communications in law firms is raising new issues. For a thorough discussion of the attorney-client privilege and the use of e-mail communications in the legal setting, see William P. Matthews, *Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 U. KAN. L. REV. 273, 285-95 (1996).

20. *See* Mitchell, *supra* note 19, at 92 (quoting Professor John Wiley of University of California at Los Angeles School of Law as stating that "[e]-mail is a rich source of information in lawsuits. . . . [and] is a window into the internal working of an organization"); *The Hidden Risks of E-Mail*, AM. LAW., Apr. 1996, at 109 ("'The basic rule is that electronic information is subject to discovery to the same extent and with the same general limits relating to relevance, privilege, and burden that paper-based information is.'" (quoting Michael Patrick, Partner, Fenwick & West)).

21. *See* Strauss v. Microsoft Corp., No. 91 Civ. 5928 (SWK), 1995 WL 326492, at *4 (S.D.N.Y. June 1, 1995) (finding executive's e-mails were relevant evidence in sexual discrimination suit).

22. *See* Owens v. Morgan Stanley & Co., No. 96 Civ. 9747 (DLC), 1997 U.S. Dist. LEXIS 10351, at *6 (S.D.N.Y. July 16, 1997) (granting defendants' motion to dismiss plaintiffs' employment discrimination and state law contract and negligent hiring claims); Susan Harrigan, *Workers File Bias Lawsuit Over E-Mail at Brokerage House*, NEWSDAY, Jan. 14, 1997, at A41; *The CNN Computer Connection* (CNN television broadcast, Jan. 18, 1997) [hereinafter *Computer Connection*]. According to the plaintiff's attorney, Howard Shafran, the e-mail "purported to be a 'homework assignment' by 'Leroy,' a public-school ninth-grader who misuses a number of words in an obscene manner apparently intended to mock [African-American] street slang." Harrigan, *supra*, at A41. In addition, the complaint filed in a United States District Court in Manhattan, New York seeks to be certified as a class action suit for all African-American employees at Morgan Stanley. *See id.*

23. *See* Harrigan, *supra* note 22, at A41; *Computer Connection*, *supra* note 22. Once Morgan Stanley executives were notified of the complaint, they took strong action against the six employees who distributed the message, which included revoking supervisory responsibilities. *See* Harrigan, *supra* note 22, at A41; *Computer Connection*, *supra* note 22. Shortly after the filing of the complaint, Morgan Stanley

United States District Court for the Southern District of New York.[24]

Second, employees often allege that their privacy rights have been violated when employers monitor their workplace e-mail communications.[25] A 1993 study found that twenty-two percent of employers searched employees' "computer files, voice mail, electronic mail, or other networking communications."[26] A more recent study found that thirty percent of 538 business executives polled admitted to randomly monitor-

issued a statement asserting that it "does not and will not tolerate any form of discrimination or harassment." Harrigan, *supra* note 22, at A41. Furthermore, a Morgan Stanley spokesperson stated that the firm's code of conduct specifically prohibits the workplace distribution of materials "containing inappropriate and offensive content," but the large size of the firm severely hampers its ability to monitor e-mail for strict compliance. *Id.* For a further discussion of situations involving e-mail messages causing companies litigation troubles, see Overly, *supra* note 18, at 75.

24. *See Racial, Ethnic Jokes Sent By E-mail Prompt Class Action Against Citibank*, DAILY LAB. REP., Feb. 26, 1997, at 38. In the complaint, two African-American Citibank employees alleged that Caucasian supervisors disseminated "vulgar and racially vile messages that demeaned and ridiculed African-American people." *Id.* Although no African-American employees received the racially offensive messages, the plaintiffs alleged that Citibank executives failed to take appropriate action once they were informed about the messages, thereby allowing a "pervasively abusive racially hostile work environment." *Id.* Citicorp, the corporate parent of Citibank, made a statement shortly after the suit was filed in federal court asserting that it had investigated the incident the day after learning about the e-mail communications. *See id.* Citicorp claimed it had taken disciplinary actions against the four Citibank employees who had distributed the e-mail; one employee was terminated, a former employee had his benefits suspended and the other two employees were suspended without pay for one month. *See id.* Furthermore, the company stated that "'[t]his specific E-mail is clearly contrary to Citicorp's stated and broadly communicated policies about use of E-mail and about providing for a workplace that is respectful of all employees.'" *Id.* (quoting Citicorp's February 21, 1997 statement); *see also* Louise Branson, *Lawsuits Show It's Not as Private as You May Think*, THE STRAITS TIMES (Singapore), Mar. 22, 1997, at 6 (stating that Morgan Stanley and Citibank lawsuits will "unleash an avalanche of cases using as evidence e-mail its senders had assumed [was] deleted"); Chrisena Coleman, *Postal Worker Hit Over Racist E-mail*, DAILY NEWS (New York), Mar. 22, 1997, at 8 (discussing suspension of United States Postal Service supervisor for circulating racist e-mail on Postal Service computer systems). For a further discussion of racial, ethnic or gender discrimination lawsuits involving e-mail communications in the workplace, see Michelle Singletary, *E-Mail Humor: Punch Lines Can Carry Prices; Jokes Open Employers to Discrimination Suits*, WASH. POST, Mar. 18, 1997, at A1 (quoting Stephen L. Sheinfeld, a New York City labor and employment attorney with Whitman, Breed, Abbott & Morgan, as stating that "[c]laimants are now searching the e-mail systems looking for smoking guns and because e-mail is unerasable, it can come back to haunt an employer").

25. *See* Donovan, *supra* note 15, at B5 ("Many people make the mistake of thinking office e-mail is as private as U.S. mail."); *see also* Mathis, *supra* note 15, at 10 ("Privacy advocates contend that e-mail monitoring creates a stressful workplace.").

26. Andrea Bernstein, *Who's Reading Your E-mail?*, NEWSDAY, July 15, 1996, at A21. This survey concluded that roughly "20 million American employees may be subject to electronic monitoring through their computers." *Id. But see* Calvey, *supra* note 17, at A11 ("[S]ome attorneys are discouraging companies from the widespread practice of monitoring employees' e-mail.").

ing their employees' e-mail communications.[27] Although employees and privacy rights advocates often claim employers overstep the bounds of allowable intrusions, employers often have legitimate business reasons for monitoring workplace e-mail communications.[28] To combat invasion of privacy, employees may be tempted to encrypt their e-mail messages.[29] This practice, however, may make an employer suspicious as to what the employee is sending over the e-mail system.[30] As one commentator recently stated in quite simple terms: "Never expect privacy for E-mail sent through a company [computer] system."[31]

Finally, another area for concern in the modern workplace is e-mail communications to and from a corporation's in-house counsel.[32] The scope and protection of the attorney-client privilege when dealing with an in-house counsel's e-mail communications is less than one might believe.[33] Such communications will be protected from discovery requests only if the communication is "clearly part of rendering legal advice."[34]

---

27. *See* Liz Halloran, *Big Brother Is Reading This; Your Boss Can Browse Your E-mail*, HARTFORD COURANT, Apr. 15, 1996, at A1. The Society for Human Resource Management, based in Virginia, conducted the poll. *See id.*

28. *See Employers Stepping Up Monitoring in Workplace* (CNN television broadcast, Sept. 1, 1996) (interviewing employers who suggest reasons to monitor e-mail of employees) [hereinafter *Employers Stepping Up*]. Hal Coxson, a Washington, D.C. attorney, cited four examples justifying employer monitoring of employees in the workplace in general: first, to monitor "employee performance-productivity, quality of work, [and] customer satisfaction;" second, to monitor for employee misconduct such as "theft, . . . drugs, gambling, [and] misuse of company property for disclosure of confidential material;" third, to protect employee safety and health; and fourth, to reduce "employer reliability for employee's acts." *Id.* Additionally, within the health services industry, employers have started to monitor their employees' e-mail messages for three reasons: to reveal improper use of the company's e-mail system, to prevent the disclosure of potentially damaging confidential patient information and to aid in evaluating employee productivity. *See* Van Doren, *supra* note 19, at 12. For a further discussion of legitimate reasons for an employer to monitor employee e-mail communications, see *infra* notes 76-87 and accompanying text.

29. For a further discussion of encryption, see Dorothy E. Denning & William E. Baugh, Jr., *Key Escrow Encryption Policies and Technologies*, 41 VILL. L. REV. 289 (1996).

30. *See* Eryn Brown, *The Myth of E-mail Privacy*, FORTUNE, Feb. 3, 1997, at 66. One employee stated that after an employer began monitoring workplace e-mail, "I was afraid that if I merely sent an encrypted letter, they'd think I was up to something bad." *Id.*

31. *Id.*

32. *See The Hidden Risks of E-Mail*, *supra* note 20, at 109 (stating that in-house counsel can act in many different capacities when sending e-mail and, thus, may or may not be protected by attorney-client privilege).

33. *See id.* Michael Patrick, a partner at Fenwick & West, believes that a corporation's in-house counsel acts in two capacities, both as a lawyer and a business executive. *See id.* While acting in these two capacities, in-house counsel can communicate over an e-mail system without distinguishing between his or her official functions. *See id.* Mr. Patrick also warns that judges often construe the attorney-client privilege narrowly so as to not "impede the search for truth." *Id.*

34. *Id.* Mr. Patrick also suggests that in-house counsel should mark all docu-

## III. SOURCES OF THE RIGHT TO PRIVACY IN THE PRIVATE EMPLOYMENT CONTEXT

### A. *The United States Constitution*

In 1965, the United States Supreme Court recognized a constitutional right to privacy in *Griswold v. Connecticut*.[35] The Constitution, however, protects an individual's privacy rights only from governmental intrusions.[36] Therefore, the United States Constitution does not offer protection to employees from the actions of private employers.[37]

### B. *State Constitutions*

Many state constitutions specifically offer privacy protection similar to the Fourth Amendment's prohibition against unlawful searches and seizures.[38] Additionally, nine states explicitly guarantee the right to privacy within their constitutions.[39] Like the Federal Constitution, eight of

---

ments "confidential, and attorney-client privileged communication." *Id.* This attempt to ensure privacy, however, can be ineffective because "the privilege can be waived if the message gets forwarded to people inside the company . . . or to outsiders." *Id.* Even though the label does not legally create a privileged document, it does serve two purposes: first, to alert recipients of the communication that this communication should be treated appropriately and, second, to notify those conducting a document review "to identify and not produce those messages that are from counsel and are subject to a claim of privilege." *Id.*

35. 381 U.S. 479 (1965). For a further discussion of *Griswold*, see *supra* note 6 and accompanying text.

36. *See* Flanagan, *supra* note 8, at 1264-65 ("The Fourth Amendment to the U.S. Constitution protects individual privacy from government intrusion. Hence, the protection of the Constitution extends only to public employees; private employer behavior toward employees is not restricted." (footnote omitted)).

37. *See* Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 394 (W.D. Okla. 1978) (refusing to extend Fourth Amendment privacy protection to employee in private workplace), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

38. *See* Flanagan, *supra* note 8, at 1265 ("Most states have a constitutional provision that reflects the proscriptions in the Fourth Amendment regarding search and seizure.").

39. *See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein."); HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. . . . Any person adversely affected by a search or seizure conducted in violation of this Section shall have

the nine states that recognize the right to privacy in their state constitutions limit its protection to public employees.[40] Of the nine states, only California extends constitutional privacy rights to both public and private employees.[41] The California Superior Court, in *Flanagan v. Epson America*,[42] however, refused to extend California's constitutional right to privacy to a private employee's e-mail communications.[43] The California court suggested that the extension of constitutional privacy rights was

standing to raise its illegality in the appropriate court."); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); *see also* State v. Gonzalez, 825 P.2d 920, 932 (Alaska Ct. App. 1992) ("Our constitutional right to privacy finds no express counterpart in the federal constitution and has thus served as the basis for extending protections to Alaska citizens that are not extended under the United States Constitution."), *aff'd*, 835 P.2d 526 (Alaska 1993); State v. Baldwin, 908 P.2d 484, 489 (Ariz. Ct. App. 1995) ("The Arizona Constitution, unlike the United States Constitution, gives explicit protection to privacy."); Wallace v. Guzman, 687 So.2d 1351, 1353 (Fla. Dist. Ct. App. 1997) ("The people have spoken" in creating right to privacy within Florida Constitution.); Hawaii Org. of Police Officers v. Society of Prof'l Journalists, 927 P.2d 386, 405 (Haw. 1996) ("'By amending the Constitution to include a separate and distinct privacy right, it is the intent of [the legislature] to insure that privacy is treated as a fundamental right for purposes of constitutional analysis.'" (quoting committee reports to constitutional convention of Hawaii)); People v. Carter, 672 N.E.2d 1279, 1285 (Ill. App. Ct. 1996) (stating "that the Illinois Constitution offers greater protection against the invasion of an individual's privacy rights than does the Federal Constitution"); State v. Davis, 684 So.2d 540, 540 (La. Ct. App. 1996) ("Louisiana Constitution affords greater protection for freedom from invasion than the Fourth Amendment of the United States Constitution does and that we, therefore, are not bound by federal jurisprudence."); John Sanchez, *Constitutional Privacy in Florida: Between the Idea and the Reality Falls the Shadow*, 18 NOVA L. REV. 775, 778 (1994) (discussing Florida's constitutional right to privacy); Timothy Stallcup, *The Arizona Constitutional "Right to Privacy" and the Invasion of Privacy Tort*, 24 ARIZ. ST. L.J. 687, 690 (1992) (discussing Arizona's constitutional right to privacy).

40. *See* Flanagan, *supra* note 8, at 1265.

41. *See* Porten v. University of S.F., 134 Cal. Rptr. 839, 842 (Ct. App. 1976) ("Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone."). In California, an employer must show that he or she has a compelling interest to overcome an employee's reasonable expectation of privacy. *See* White v. Davis, 533 P.2d 222, 234-35 (Cal. 1975) (holding employee had constitutional privacy claim against employer who could not prove compelling interest); Luck v. Southern Pac. Trans. Co., 267 Cal. Rptr. 618, 632 (Ct. App. 1990) (holding private train company did not prove compelling interest for drug testing). For a further discussion of state constitutional privacy protection, see Julia Turner Baumhart, *The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923, 943-45 (1992).

42. No. BC007036 (Cal. Super. Ct. Jan. 4, 1991). For a discussion of the *Flanagan* case, see Frank C. Morris et al., *Issues from the Electronic Workplace and E-mail Communication: The Developing Employment Law Nightmare*, SB07 A.L.I.-A.B.A. 335, 341 (1996).

43. *See* Morris et al., *supra* note 42, at 343. The court further rejected the employer's contention that federal wiretap statutes preempted a private employee's state constitution-based privacy claim. *See id.* For a further discussion of federal wiretap statutes, see *infra* notes 54-93 and accompanying text.

within the province of the California legislature, not the California judiciary.[44]

### C. *Common Law*

An employee could successfully bring a common law cause of action against a private employer when the employer obtains access to the employee's workplace e-mail. There are two common law causes of action in this situation: the privacy tort of intrusion upon seclusion and intentional infliction of emotional distress.

First, the employee may bring an invasion of privacy cause of action against the employer for intrusion upon seclusion.[45] The intrusion upon seclusion tort is defined as follows: "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."[46] If an employee is to succeed in bringing this action, he or she has to prove that an employer's access to the e-mail communications was a "highly offensive [intrusion] to a reasonable person."[47] One commentator has stated that "if [an] employer obtains information about [the employee] through the employer's . . . computer system . . . [the employee] will have much greater difficulty in winning a[n invasion of privacy] lawsuit."[48] As a result, an employee usually does not succeed when bringing

44. *See* Morris et al., *supra* note 42, at 343.

45. *See* HENRY H. PERRITT, JR., WORKPLACE TORTS: RIGHTS AND LIABILITIES 202 (1991). In 1960, Dean William L. Prosser set forth the intrusion upon seclusion tort as one of four right to privacy torts. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (describing tort as "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs"). Dean Prosser's four privacy torts, intrusion upon seclusion, public disclosure of private facts, false light and appropriation, were later incorporated into the *Restatement (Second) of Torts*. *See* TURKINGTON ET AL., *supra* note 1, at 49; *see also* Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 671 (1996) ("Two well-established common law doctrines increasingly are coming into conflict. The first protects individuals from unreasonable intrusions on their privacy. The second authorizes an employer to fire its employees at will, unless a clear agreement exists to the contrary.").

46. RESTATEMENT (SECOND) OF TORTS § 652B (1965). One must also establish that the "subjective expectation of privacy" was "objectively reasonable." PERRITT, *supra* note 45, at 203. Consequently, the individual must show a subjective expectation of privacy "tested by outward manifestations that the claimant expected the information to remain private." *Id.*

47. RESTATEMENT (SECOND) OF TORTS § 652B.

48. HENRY H. PERRITT, JR., YOUR RIGHTS IN THE WORKPLACE 140 (1993). In addition, Flanagan stated that an employee must overcome three major obstacles to be successful in an intrusion upon seclusion tort claim. *See* Flanagan, *supra* note 8, at 1267. First, the employee must show that the workplace is a "sufficiently private atmosphere." *Id.* Second, the employee must prove that the e-mail intrusion was highly objectionable to the reasonable person. *See id.* Third, the employee must contend with jurisdictions that require the publication of the information learned during the privacy intrusion. *See id. But see* Dietemann v. Time, Inc., 449

an intrusion upon seclusion claim against his or her employer for e-mail monitoring.[49]

Second, an employee may bring a claim against his or her employer for intentional infliction of emotional distress resulting from e-mail monitoring in the workplace.[50] In defining the tort of intentional infliction of emotional distress, the *Restatement (Second) of Torts* states that "[o]ne who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to another results from it, for such bodily harm."[51] Although this tort could be available to an employee, it is unlikely that a court would characterize an employer's access to an employee's e-mail to be "extreme and outrageous conduct."[52] Therefore, except in the most "extreme and outrageous" circumstances, an employee's intentional infliction of emotional distress cause of action would most likely fail.[53]

### D. *Federal Statutory Enactments*

#### 1. *The Electronic Communication Privacy Act of 1986*

The United States Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA)[54] to amend the technologically antiquated Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("OCCSSA").[55] Congress realized that the existing laws protecting business and

F.2d 245, 247 (9th Cir. 1971) (holding that publication is not necessary element of intrusion upon seclusion).

49. *See* Flanagan, *supra* note 8, at 1267 ("The combination of these requirements typically defeats the employee's tort claim."). For a discussion of a recent federal district court case decided under the intrusion upon seclusion tort framework, see *infra* notes 102-08 and accompanying text.

50. *See* Flanagan, *supra* note 8, at 1267 n.82 ("An employee might claim that the employer's violation of privacy constitutes the tort of intentional infliction of emotional distress rather than invasion of privacy.").

51. RESTATEMENT (SECOND) OF TORTS § 46. Dean Prosser further defined the tort of intentional infliction of emotional distress as follows: "[T]he rule which seems to have emerged is that there is liability for conduct exceeding all bounds usually tolerated by decent society, of a nature which is especially calculated to cause, and does cause, mental distress of a very serious kind." WILLIAM PROSSER, LAW OF TORTS 56 (4th ed. 1971).

52. *See* Flanagan, *supra* note 8, at 1267 n.82 ("[T]he employer's conduct must be extreme in degree, outrageous in character, and 'atrocious, and utterly intolerable in a civilized community.'" (quoting Kaminski v. United Parcel Serv., 501 N.Y.S.2d 871, 873 (App. Div. 1986))).

53. *See* Blackburn et al., *supra* note 7, at 56 n.54 (stating that emotional distress tort "places severe restrictions to recovery upon an employee whose privacy has been invaded" and is usually unhelpful in workplace privacy suit).

54. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

55. 18 U.S.C. §§ 2510-2520 (1994). The United States Congress enacted Title III of the OCCSSA in response to the United States Supreme Court's decision in *Berger v. New York*, 388 U.S. 41 (1967). *See* S. REP. No. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555. In *Berger*, the Supreme Court, for the first time, pro-

personal communications had "not kept pace with the development of communications and computer technology. Nor [had the laws] kept pace with changes in the structure of the telecommunications industry."[56] In amending Title III of the OCCSSA, Congress sought to "bring it in line with technological developments and changes in the structure of the telecommunications industry."[57] In its discussion of technological advancements, Congress specifically mentioned that e-mail required additional protection.[58]

---

tected oral conversations from electronic eavesdropping under the Fourth Amendment to the United States Constitution. *Berger*, 388 U.S. at 55-64.

56. *See* S. REP. NO. 99-541, at 2. The Senate Report to the ECPA ("Senate Report") also acknowledged that since the enactment of the Constitution, "development of new methods of communication and devices for surveillance [had] expanded dramatically the opportunity for . . . intrusions" into Fourth Amendment protected areas. *See id.* at 1-2. In addition, Senator Patrick Leahy, a sponsor of the ECPA, stated that Title III of the OCCSSA was "hopelessly out of date." 132 CONG. REC. 7992 (1986) (statement of Sen. Leahy).

57. S. REP. NO. 99-541, at 3. In recognizing the inherent risks of the technological revolution, the Senate Report stated that:

> These tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.

*Id.* As a result of this concern, Congress stated that under the ECPA, "[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances." *Id.* at 5. Furthermore, Congress felt it had to "act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right." *Id.*

58. *See id.* at 3-4. Senator Leahy requested a determination in 1984 from the United States Attorney General concerning the protection status of e-mail communications under the then existing Title III of the OCCSSA. *See id.* at 3. The Department of Justice (DOJ) responded to Senator Leahy's query, and stated that "[f]ederal law protects electronic communications against unauthorized acquisition only where a reasonable expectation of privacy exists." *Id.* at 4. Under this standard, the DOJ concluded that specific legislation was required for such communications because determining whether a reasonable expectation of privacy exists was "not always clear or obvious." *Id.* In addition, in October 1985, Congress's Office of Technology Assessment concluded in a study that e-mail protection at that time was "weak, ambiguous, or non-existent . . . [and that] electronic mail remains legally as well as technically vulnerable to unauthorized surveillance." OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 31 (1985).

During the enactment of the ECPA, the Senate Report clearly described many of the new telecommunications and computer technologies including electronic mail, cellular telephones, electronic pagers and remote computer services. S. REP. NO. 99-541, at 8-10. The Senate Report described electronic mail in the following manner:

> Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box"

a. Access to Stored E-Mail: Title II of the ECPA

The focus of analysis will be on the Stored Wire and Electronic Communications and Transactional Records Access ("Stored Communications Act")[59] provisions, or Title II of the ECPA.[60] More specifically, cases involving employer access to stored e-mail messages are governed by 18 U.S.C. § 2701.[61] Under § 2701, a person or entity violates the Stored Communications Act if he or she "intentionally accesses without authorization a facility through which an electronic communication service is provided."[62] Courts must sanction a violation of the Stored Communications Act for "commercial advantage, malicious destruction or damage, or private commercial gain" with more severity than other violations.[63]

The Stored Communications Act provides two exceptions for the access of stored e-mail communications: the provider exception and the user exception.[64] First, under the provider exception, the Stored Communica-

until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.

*Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.*

*Id.* at 8 (emphasis added).

59. 18 U.S.C. §§ 2701-2711 (1994).

60. *See id.* §§ 2510-2711. The Senate Report modeled this portion of the ECPA after the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1994). *See* S. REP. NO. 99-541, at 3 (stating purpose was to "protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs"). Under amended Title III of the OCCSSA, "electronic storage" is defined as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

61. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462-63 (5th Cir. 1994) (holding that seizure of stored electronic communications is governed by Title II of ECPA). For a further discussion of *Steve Jackson Games*, see *infra* notes 88-93 and accompanying text.

62. 18 U.S.C. § 2701(a)(1). In addition, an individual violates the Stored Communications Act if he or she "intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." *Id.* § 2701(a)(2).

63. *Id.* § 2701(b). If an individual is convicted of violating the Stored Communications Act for the above defined purposes, the punishment is "(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense . . . ; and (B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense." *Id.* § 2701(b)(1). If an individual violates the Stored Communications Act for any other purpose, the punishment is "a fine under this title or imprisonment for not more than six months, or both." *Id.* § 2701(b)(2).

64. *Id.* § 2701(c). A discussion of the Stored Communications Act's third exception, the governmental access exception described within § 2701(c)(3), is beyond the scope of this Comment.

tions Act does not apply to conduct authorized "by the person or entity providing a wire or electronic communications service."[65] According to many commentators who interpret the provider exception broadly, private employers who maintain a computer system have the ability to peruse and disclose employee e-mail communications without violating the Stored Communications Act.[66] Other commentators have recommended that employers should be cautious when justifying their monitoring of e-mail with the provider exception.[67] Some commentators warn, however, that employers should not rely extensively on the provider exception if the employer merely provides a common carrier's e-mail service to its employees.[68] Second, under the user exception, the Stored Communications Act

65. *Id.* § 2701(c)(1). One commentator has noted that "it may reasonably be contended that employers have the right to search in-house E-mail under [the ECPA] because such communications, if limited to exchanges of employer information, may constitute the employer's property, which the employer retains the right to supervise." JAMES BAIRD ET AL., PUBLIC EMPLOYEE PRIVACY: A LEGAL AND PRACTICAL GUIDE TO ISSUES AFFECTING THE WORKPLACE 60 (1995). Other commentators have determined that the ECPA provides a much greater cloak of immunity for employers because "[c]ompany snooping and Big Brotherism is not a felony or even a misdemeanor under the ECPA. It is entirely legal." Joanne Goode & Maggie Johnson, *Putting Out the Flames: The Etiquette and Law of E-Mail*, ONLINE, Nov. 1991, at 61.

66. *See* Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 359 (1995) (citing various commentators who support broad interpretation of Stored Communications Act's provider exception). One commentator has asserted that the Stored Communications Act is inapplicable to employers because they are not a "third party" accessing the stored e-mail communication. *See* Steven B. Winters, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail*, 1 S. CAL. INTERDISC. L.J. 85, 116-19 (1992). Gantt suggested that this assertion is "imprecise because employers are 'third parties' to employee-employee communications." Gantt, *supra*, at 359 n.96.

67. *See* Baumhart, *supra* note 41, at 925. Baumhart contends that "to blindly adopt the view that the [ECPA] imposes no access limitations on employers who possess their own systems ignores Congress' stated intent to procure parity in the protection of personal communications." *Id.* at 926. In addition, Baumhart stated that by "[a]dopting [the broad interpretation] of the provisions, a 'corporate big brother' is free to read at leisure employee E-mail messages, *no matter how personal.* Moreover, the employer then has almost unfettered discretion to disclose the contents of a message." *Id.* (emphasis added). Baumhart conceded, in arguing for a more restrictive application of the provider exception, that most of the testimony from a Senate hearing on the ECPA "reflected an overriding concern for company, rather than individual employee privacy." *Id.*

68. *See* Gantt, *supra* note 66, at 360 & nn.101-02 (listing common carriers of e-mail communications services such as Prodigy, CompuServe, AT&T Mail, SprintMail and MCI Mail); *see also* Theodora R. Lee, *Privacy Issues in the Workplace, in* WRONGFUL TERMINATION CLAIMS: 1996, at 411, 462 (PLI Litig. & Admin. Practice Course Handbook Series No. 558, 1997) ("[E]mployers may not access messages if the system is provided by an outside entity such as MCI Mail without the authorization of either the employee who communicated the message or the intended receiver of the message."). *But see* Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 899 (1996) (asserting that "[t]he ECPA only protects messages sent over public networks such as MCI mail, Internet, Prodigy, or CompuServe because the definition of 'electronic com-

does not apply to conduct authorized "by a user of that service with respect to a communication of or intended for that user."[69] One commentator asserts that such authorization "may be expressly given, and in some cases, reasonably implied from the surrounding situation."[70]

b. Interception of E-Mail: Title III of the OCCSSA as Amended by Title I of the ECPA

The interception[71] of an e-mail communication is governed by Title III of the OCCSSA.[72] Through Title I of the ECPA, Title III of the OCCSSA was amended to extend interception protection to "electronic communication."[73] Under 18 U.S.C. § 2511, an individual violates Title III of the OCCSSA if he or she "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or *electronic communication.*"[74] Damages for a violation of Title III of the OCCSSA are more severe than damages for a violation of the Stored Communications Act.[75]

---

munication' . . . pertains to a communication that 'affects interstate or foreign commerce'" (quoting 18 U.S.C. § 2510(12) (1994))). Hash and Ibrahim suggest that the ECPA may not cover intracompany e-mail unless the employer's system "crosses state lines or perhaps connects to an interstate network." *Id.* In addition, they state that the ECPA is unclear on this point and judicial interpretation is necessary to determine whether intracompany e-mail has ECPA protection. *See id.*

69. 18 U.S.C. § 2701(c)(2) (1994).

70. Sally D. Garr, *Employee Monitoring in the Internet Age*, SB53 A.L.I.-A.B.A. 11 (1997) (stating that standard for determining whether access was given is similar to standard of consent under 18 U.S.C. § 2511(2)(d), dealing with interception of wire, oral or electronic communications). For a discussion on consent to e-mail interception, see *infra* notes 85-87 and accompanying text.

71. *See* 18 U.S.C. § 2510(A) (1994) (defining interception as "the aural or other acquisition of the contents of any wire, *electronic*, or oral communications through the use of any electronic, mechanical, or other device" (emphasis added)).

72. 18 U.S.C. §§ 2510-2521; *see* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994). For a further discussion of *Steve Jackson Games*, see *infra* notes 88-93 and accompanying text.

73. *See* S. REP. NO. 99-541, at 14 (1986); *see also* Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 232 n.70 (1994) ("The addition of 'electronic communication' to Title III opened the door for the protection of a host of modern communication technologies not covered prior to 1986."). Prior to the passage of the ECPA, Title III of the OCCSSA protected "only communications capable of being heard" from interception. BAIRD ET AL., *supra* note 65, at 59.

74. 18 U.S.C. § 2511(1)(a) (1994) (emphasis added).

75. *See* Baumhart, *supra* note 41, at 936. If an individual's wire, oral, or electronic communication is unlawfully intercepted, he or she is entitled to "(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages . . . and punitive damages in appropriate cases; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred." 18 U.S.C. § 2520(b) (1994). Damages for unlawfully intercepted electronic communications are determined as follows: a first time violator is liable for the greater of actual damages or statutory damages, not less than $50 and not greater than $500; a two-time violator is liable for the greater of actual damages or statutory damages, not less than $100

Like the Stored Communications Act, Title III of the OCCSSA has exceptions that create allowable interceptions of wire, oral or electronic communications.[76] The ordinary course of business exception is found buried within Title III's definition section.[77] Under this exception, an employer may intercept an employee's e-mail communications in the ordinary course of its business if it uses "equipment or [a] facility, or any component thereof" furnished by the provider of the electronic communication service in the ordinary course of its business.[78]

One commentator has separated cases dealing with employer liability under the ordinary course of business exception of Title III of the OCCSSA into two distinct branches: "legitimate business purpose" cases and "subject of the call" cases.[79] Cases involving the legitimate business purpose exception focus upon whether the employer had a legitimate business purpose to justify the interception of the employee's communication.[80] Courts have held that telephone monitoring to ensure better quality control[81] and to reduce personal use was an allowable inter-

---

and not greater than $1000; and any other violator is liable for the greater of "the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation" or "statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000." *Id.* § 2520(c).

76. *See* 18 U.S.C. § 2520(d). Section 2520 provides three good faith defenses to liability under Title III of the OCCSSA. *See id.* Section 2520(d) states that:

> A good faith reliance on —
>
> (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; or
>
> (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
>
> (3) a good faith determination that section 2511(3) of the title permitted the conduct complained of;
>
> *is a complete defense* against any civil or criminal action brought under this chapter or any other law.

*Id.* (emphasis added).

77. *See id.* § 2510(5)(a) (defining "electronic, mechanical, or other device").

78. *Id.* Section 2510(5)(a) provides in part that:

> "[E]lectronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication *other than* —
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the *ordinary course of its business* and being used by the subscriber or user in the *ordinary course of its business* or furnished by such subscriber or user for connection to the facilities of such service and used in the *ordinary course of its business* . . . .

*Id.* (emphasis added).

79. *See* Greenberg, *supra* note 73, at 239.

80. *See id.* When determining whether a legitimate business purpose exists, a court must look to whether: "(1) the employer had a reasonable business justification for the intrusion; (2) employees were provided notice of the possibility of monitoring; and (3) the employer acted consistently with respect to the extent of the monitoring of which employees were warned." *Id.* at 239 n.104.

81. *See* James v. Newspaper Agency Corp., 591 F.2d 579, 581 (10th Cir. 1979)

ception under Title III's ordinary course of business exception.[82]

The "subject of the call" cases establish "the basic rule that calls relating to the business of the employer may be intercepted."[83] Following this rationale, an employer is not allowed to monitor personal telephone communications, except to the extent necessary to determine whether they are personal and not business related.[84]

Under either Title III of the OCCSSA or the Stored Communications Act, the employer may raise the defense of consent, whereby the employee consented to either the e-mail interception or access to stored e-mail.[85] Courts will uphold the consent defense if the employee's consent is found to be either express or implied.[86] By proving implied consent through a well-disseminated e-mail policy, the likelihood of an employer's liability is decreased.[87]

---

(holding that, after providing notice, employer could intercept telephone communications to help employees provide better service).

82. *See* Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 397 (W.D. Okla. 1978) (holding that, after providing notice, employer could monitor telephone switchboard and then discharge employee for using telephone for personal reasons).

83. Greenberg, *supra* note 73, at 241.

84. *See* Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (noting that personal call may be intercepted to determine its nature in ordinary course of business); Epps v. St. Mary's Hosp., 802 F.2d 412, 417 (11th Cir. 1986) (holding monitoring conversation between hospital employees was within ordinary course of business); Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983) (holding that monitoring of personal calls was not in ordinary course of business); Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (holding that employer may monitor telephone calls based upon fear of disclosure of sensitive business information); Greenberg, *supra* note 73, at 241 ("[P]ersonal calls cannot be intercepted, except to the extent necessary to determine whether or not the call is personal.").

85. *See* 18 U.S.C. § 2511(2)(d) (1994); 18 U.S.C. § 2701(a)(1) (1994).

86. *See* Mark J. Manta, *Electronic Surveillance and Employee Privacy in the Workplace*, METROPOLITAN CORP. COUNS., June 1996, at 16 ("The ECPA allows the interception of electronic communications where one of the parties to the communication has given prior consent, express or implied, to such an interception."); *see also* Gantt, *supra* note 66, at 356 (stating that "courts have held that consent under the interception exception may be implied or actual, but that constructive consent is inadequate"). Some commentators suggest that although courts have not yet interpreted the Stored Communication Act's consent defense when courts are faced with the issue, they will treat it in a manner similar, if not identical, to the consent defense in § 2511(2)(d). *See id.*; *see also* Garr, *supra* note 70, at 11 ("Furthermore, although the courts have not yet interpreted the consent exception under the stored communications provisions, courts have held that consent . . . may be implied or actual.").

87. *See* Gantt, *supra* note 66, at 356 (stating that court in *Watkins* limited employee consent to confines of employer monitoring policy). For a further discussion of e-mail policies in the workplace and their effects on employer liability, see *infra* notes 121-48 and accompanying text.

### 2. *Judicial Interpretation of the ECPA:* Steve Jackson Games, Inc. v. United States Secret Service

One commentator has recently noted that the ECPA "is ambiguous and has not yet been clarified through case law."[88] The United States Court of Appeals for the Fifth Circuit, however, addressed the privacy issue concerning stored electronic communications under the ECPA in *Steve Jackson Games, Inc. v. United States Secret Service.*[89] The Fifth Circuit sought to determine whether the federal government intercepted e-mail communications stored on a private e-mail system in violation of 18 U.S.C. § 2511(1)(a) under Title I of the ECPA.[90] The court held that the United States Secret Service did not intercept the stored e-mail in violation of Title I, but that the Secret Service did unlawfully access the stored e-mail

88. Connie L. Michaels, *Employment Law Considerations, Stress Management, and Elimination of Bias: The Risk Management Perspective, in* CONDUCTING EMPLOYEE INVESTIGATIONS: LEGAL PARAMETERS AND PRACTICAL SUGGESTIONS: 1996, at 289 (PLI Litig. & Admin. Practice Course Handbook Series No. 555, 1996).

89. 36 F.3d 457 (5th Cir. 1994).

90. *See id.* at 460. Steve Jackson Games, Inc., the appellant, operated an electronic bulletin board system ("BBS") to disseminate information to the public about its publishing business. *See id.* at 458. In addition, the appellant provided a private e-mail service to its 365 BBS users. *See id.* The court noted: "Private E-mail was stored on the BBS computer's hard disk drive temporarily, until the addressees 'called' the BBS (using their computers and modems) and read their mail. After reading their E-mail, the recipients could choose to either store it on the BBS computer's hard drive or delete it." *Id.* In March 1990, the United States Secret Service executed a warrant to search the appellant's premises for alleged evidence relating to an "unauthorized duplication and distribution of a computerized text file, containing information about [the Bell Company's] emergency call system." *Id.* at 458-59. The search warrant authorized the seizure of the following:

> Computer hardware . . . and computer software . . . and . . . documents relating to the use of the computer system . . . and financial documents and licensing documentation relative to the computer programs and equipment at . . . [Steven Jackson Games, Inc.] . . . which constitute evidence . . . of federal crimes . . . . This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data.

*Id.* at 459 (alterations in original). Pursuant to this search, the Secret Service confiscated, and later read and deleted, "162 items of unread, private E-mail . . . stored on the BBS." *Id.*

The appellant filed suit in federal court against the Secret Service and the United States under the Federal Wiretap Act and the ECPA. *See id.* The district court found for the appellant, holding that the Secret Service unlawfully seized the stored e-mail communications in violation of the ECPA. *See id.* The court awarded each user of the appellant's system $1000 for statutory damages under Title II of the ECPA, $195,000 for attorneys' fees and $57,000 in costs. *See id.* Although the court found for the appellant, it also held that the Secret Service did not intercept the e-mail communications in violation of Title I of the ECPA because the acquisition "was not contemporaneous with the transmission of those communications." *Id.* at 459-60. The Secret Service did not appeal the court's ruling, but the appellant challenged the decision, seeking the recovery of a greater damage award under Title I. *See id.* at 462-63.

in violation of 18 U.S.C. § 2701(a)(1) under Title II.[91] In reaching its decision, the Fifth Circuit stated that stored electronic communications, such as e-mail, could not be intercepted for purposes of protection under Title I of the ECPA.[92] The court concluded that access to stored electronic communications is governed solely by Title II of the ECPA.[93]

## IV. RECENT CASE LAW INVOLVING E-MAIL PRIVACY IN THE WORKPLACE

Because of the relatively recent widespread introduction of e-mail systems into the workplace, few cases exist involving an employee's right to privacy concerning e-mail communications. In 1996, two federal district courts and one state court addressed the issue of e-mail privacy in the employment context.[94]

---

91. *See id.* at 461-64. The appellant sought to distinguish its case from a case in which the Fifth Circuit defined an intercept under § 2511 to require "'participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device.'" *Steve Jackson Games*, 36 F.3d at 460 (quoting *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976)). The appellant claimed that, regardless of the *Turk* holding, an intercept still occurred because the Secret Service acquired the e-mail prior to its delivery and also prevented its delivery. *See id.* Conversely, the government argued the district court had correctly concluded that Title II of the ECPA governed the access of stored e-mail communications, not Title I. *Id.* at 461.

92. *See Steve Jackson Games*, 36 F.3d at 461-62. The court quickly rejected the appellant's argument distinguishing *Turk*, and instead relied primarily upon the language of Titles I and II of the ECPA. *See id.* at 461. The court noted that Title I defines electronic communication to specifically exclude "'electronic storage of such communications.'" *Id.* (quoting 18 U.S.C. § 2510(12) (1994)). From this statutory language, the court concluded that the "[e]-mail in issue was in 'electronic storage'" and was therefore governed by Title II of the ECPA. *Id.* In addition, the Fifth Circuit stated that the ECPA's legislative history supported its finding that stored e-mail communications could not be intercepted. *See id.* at 462.

93. *See id.* at 462-63. The Fifth Circuit further distinguished between Title I and Title II when it held that there was "no indication in either the [ECPA] or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I." *Id.* First, the court noted that a court order is required for the intercept of an electronic communication while only a warrant is required to access electronic communications stored for fewer than 180 days. *See id.* at 463. Second, the court stated that the requirements of the court order authorizing the intercept of electronic communications governing minimization, duration and the types of crimes that may be investigated do not apply to the access of stored electronic communications. *See id.* Third, the court recognized that a court order governing the intercept of electronic communications must include "strict requirements as to duration," but "[t]here is no such requirement for access to stored communications." *Id.* Fourth, the court noted that Title II contains no limitations as to the types of crimes to be investigated during the access of stored communications, such as those crimes that limit the applicability of a lawful intercept under Title I of the ECPA. *See id.* In addition, the court concluded that stored electronic communications are treated differently than stored wire communications because "[a]ccess to stored electronic communications may be obtained pursuant to a search warrant, 18 U.S.C. § 2703; but, access to stored wire communications requires a court order pursuant to § 2518." *Id.* at 464.

94. Bohach v. City of Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (hold-

The United States District Court for the District of Nevada decided the most recent employment e-mail privacy case in *Bohach v. City of Reno*.[95] In *Bohach*, the plaintiffs, two Reno, Nevada police officers, claimed that the City of Reno had violated the federal wiretapping statutes and their constitutional right to privacy when it (1) stored messages sent over an "Alphapage" message system[96] and (2) accessed the stored messages from police department computer files.[97]

---

ing that plaintiffs suffered no constitutional injury under Fourth Amendment or under federal wire tapping statutes when their employer accessed their e-mail messages); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding employee had no wrongful discharge claim when employer accessed employee's work-related e-mail communications); Restuccia v. Burk Tech. Inc., No. 95-2125 (Mass. App. Ct. 1996) (reversing summary judgment for employer and allowing employees to bring claims against employer who discharged them after reading their e-mail), *reprinted in The Week's Opinions; Superior Court, Massachusetts Lawyers Weekly*, Dec. 16, 1996, at 16.

95. 932 F. Supp. 1232 (D. Nev. 1996).

96. *See id.* at 1233. The Reno Police Department installed the "Alphapage" system to "allow the broadcast of 'mini news releases' and other 'timely information' to the media by means of . . . pagers . . . and thus free up the Department's regular telephone lines." *Id.* at 1234. Alphapage was a computer software program designed to transmit short alphanumeric messages or voice messages to visual display pagers from either a telephone, a stand-alone keyboard or a Local Area Network (LAN) computer. *See id.* at 1233-34. The present case involved solely the transmission of alphanumeric messages from a LAN computer to a recipient's pager. *See id.* at 1234. The district court described the technical operation of such transmission as follows:

> The user logs on to any Reno Police Department computer terminal and selects Alphapage from the menu of available functions, and then selects, from a list of all persons to whom pagers have been issued [including the press and police personnel], the name of the person to whom the message is to be sent. The user then types the message and hits the "send" key. The message is sent to the computer system's "Inforad Message Directory," where it is stored in a server file, and the user receives a message on the computer screen indicating that the page is being processed. The computer then dials the commercial paging company, sends the message to the company by modem, and disconnects. The user receives a "page sent" message on the computer screen, and the paging company takes over, sending the message to the recipient pager by radio broadcast.

*Id.* The court later stated in its discussion that it considered an Alphapage message to be "essentially electronic mail." *Id.*

97. *See id.* at 1233. The Reno Police Department had initiated an internal affairs investigation against the two plaintiffs based upon Alphapage messages sent to each other in early 1996. *See id.* The plaintiffs filed this lawsuit against the City of Reno in an effort to end the investigation and prevent the disclosure of the Alphapage messages. *See id.* The district court initially issued a temporary restraining order barring the disclosure of the messages. *See id.* After conducting a hearing, the district court dissolved the restraining order and denied the plaintiffs' request for a preliminary injunction. *See id.* In response, the plaintiffs filed an interlocutory appeal, and sought to suspend the court's injunction pending the resolution of the appeal under Rule 62(c) of the Federal Rules of Civil Procedure. *See id.* The court stated that such a request would prevent the police department from conducting an internal affairs investigation. *See id.* Because of this effective "interference by a federal court in the internal operations of a state or local gov-

First, the district court held that the plaintiffs suffered no constitutional injury under the Fourth Amendment because they had no reasonable expectation of privacy when using the Alphapage message system.[98] The court noted that any subjective expectation of privacy was unreasonable because (1) the police department notified all Alphapage users that their messages would be stored on the network; (2) the department prohibited certain types of messages from being broadcast via Alphapage and (3) the Alphapage system was easily accessible to anyone with access to the department's computer system.[99]

Second, the district court held that the plaintiffs did not have a claim under federal wiretapping statutes because no interception of electronic communications occurred, and the city, as the provider of computer service under the ECPA, could lawfully access any stored electronic communication on its Alphapage system.[100] The district court denied the plaintiffs' motion to prevent access to the stored Alphapage messages.[101]

The United States District Court for the Eastern District of Pennsylvania addressed an employee's e-mail privacy rights in *Smyth v. Pillsbury Co.*[102] In *Pillsbury*, the district court sought to determine whether an employee had a claim for wrongful discharge against the Pillsbury Company

---

ernment," the court provided Reno with the opportunity to respond to the plaintiffs' Rule 62(c) motion. *Id.*

98. *See id.* at 1234. The court determined that the plaintiffs did have a subjective expectation of privacy because "had they thought otherwise, they would [not] have sent over the system the sorts of messages they did send." *Id.*

99. *See id.* at 1235. The court further explained that no one in the police department intentionally tapped the message system because the Alphapage software itself was designed to record and store messages. *See id.* at 1234. In addition, the plaintiffs attempted to liken their communications to private telephone calls. *See id.* at 1235. The court noted, however, that for Fourth Amendment purposes, such telephone recordings were permissible because they were part of the "'ordinary course of business' for police departments." *Id.* The court distinguished the Alphapage system from a telephone by stating that "the system is not designed to communicate with the public generally" and only a person with an Alphapage pager can receive messages. *See id.* The court concluded that "one should expect, when using [Alphapage], less privacy than one might expect when . . . making a private telephone call, even from a police station." *Id.*

100. *See id.* at 1236. The court noted that federal statutes distinguish between the interception of electronic communications and the retrieval of stored electronic communications. *See id.* at 1235-36. Additionally, the court stated that once an electronic communication is stored, it cannot be intercepted; therefore, such a claim must be decided under Title II of the ECPA and not Title I. *See id.* at 1236. The court concluded that the plaintiffs did not have a valid claim against the city for the unlawful access of stored electronic communications because 18 U.S.C. § 2701(c)(1) "allows service providers to do as they wish when it comes to accessing communications in electronic storage." *Id.*

101. *See id.* at 1237. The court additionally stated that the "court's prior order . . . enjoining the City's actions pending further ORDER of this court, is VACATED, and the City is free to proceed." *Id.* (citation omitted). For a further discussion of *Bohach*, see Bernard Mower, *Privacy Rights: Search of Computerized Messages Held Outside of Worker Privacy Rights*, DAILY LAB. REP., Aug. 2, 1996, at 149.

102. 914 F. Supp. 97 (E.D. Pa. 1996).

after Pillsbury accessed the employee's work-related e-mail communications.[103] The plaintiff relied upon *Borse v. Piece Goods Shop, Inc.*[104] to support its proposition that a tortious invasion of privacy may be a sufficiently clear mandate of public policy to bar an at-will employment discharge.[105] The district court noted, however, that the *Borse* decision supported such a proposition only if an employer's invasion of privacy was "substantial and . . . highly offensive to the 'ordinary reasonable person.'" Applying this standard, the court first determined that the plaintiff did not have a reasonable expectation of privacy in the workplace e-mail communications.[106] Second, the court concluded that no reasonable person would

103. *Id.* at 98. Pillsbury provided an e-mail service to its employees "in order to promote internal corporate communications between its employees." *Id.* According to the plaintiff's complaint, Pillsbury led its employees to believe that all e-mail communications were privileged and confidential. *See id.* In addition, Pillsbury stated that it would not intercept an employee's e-mail communications or use intercepted e-mail against employees as a grounds for dismissal. *See id.* In October 1994, the plaintiff's Pillsbury supervisor sent e-mail to the plaintiff on Pillsbury's e-mail system. *See id.* The plaintiff alleged in his complaint that he replied to his supervisor's communications in reliance on Pillsbury's assurances regarding e-mail privacy. *See id.* Subsequently, Pillsbury "intercepted" these "private e-mail messages" from the plaintiff to his supervisor. *Id.* In January 1995, Pillsbury terminated the plaintiff's employment for sending "inappropriate and unprofessional comments" on its e-mail system. *See id.* at 98-99.

The plaintiff filed a diversity action in federal court against Pillsbury for wrongful discharge. *See id.* at 98. Pillsbury moved to dismiss the plaintiff's action under Rule 12(b)(6) of the Federal Rules of Civil Procedure alleging the plaintiff had failed to state a claim for which relief could granted. *See id.* Pillsbury contended in its motion that the e-mail communications "concerned sales management and contained threats to 'kill the backstabbing bastards' and referred to the planned Holiday party as the 'Jim Jones Koolaid affair.'" *Id.* at 98 n.1.

104. 963 F.2d 611 (3d Cir. 1992).

105. *See Pillsbury*, 914 F. Supp. at 100. In relying upon *Borse*, the plaintiff sought to establish that the Third Circuit would consider the tortious invasion of privacy to definitively violate a clear mandate of Pennsylvania's public policy. *See id.* Pennsylvania is an at-will employment jurisdiction and, therefore, its law does not provide a cause of action for the wrongful discharge of an at-will employee. *See id.* at 99. Under the at-will employment doctrine, an employer may fire an at-will employee "'with or without cause, at pleasure'" unless the termination "threatens or violates a clear mandate of public policy." *Id.* (quoting Henry v. Pittsburgh & Lake Erie R.R. Co., 21 A. 157, 157 (1891)). The court additionally noted that the clear mandate of public policy must "'strike[ ] at the heart of a citizen's social right, duties, and responsibilities.'" *Id.* (quoting Novosel v. Nationwide Ins. Co., 721 F.2d 894, 899 (3d Cir. 1983)).

106. *See id.* at 101. The court distinguished the present privacy intrusion from those in which a person has a reasonable expectation of privacy, namely urinalysis and personal property searches. *See id.* In addition, the court further differentiated this case because the Pillsbury executives did not require the plaintiff to disclose any personal information, as would have been the case in the urinalysis and personal property search cases. *See id.* The court determined that the e-mail communications did not enjoy a reasonable expectation of privacy even though Pillsbury had made assurances to its employees that employee e-mail would not be intercepted. *See id.* Once the plaintiff voluntarily transmitted the communication to another individual, his supervisor, the court concluded that "any reasonable expectation of privacy was lost." *Id.*

find Pillsbury's actions to be a substantial and highly offensive invasion of an employee's privacy interests.[107] The district court, therefore, granted Pillsbury's motion to dismiss.[108]

At the state level, a Massachusetts appellate court ruled on a trial court's grant of a summary judgment motion in favor of the employer in *Restuccia v. Burk Technology, Inc.*[109] In *Restuccia*, an employer discharged two employees after reading their e-mail messages stored in the employer's back-up computer files.[110] The trial court granted summary judgment for the employer on most counts, including violations of the state wiretap law, intentional infliction of emotional distress, tortious interference with contractual relations, wrongful termination, invasion of privacy, negligent infliction of emotional distress and loss of consortium.[111] The superior court reversed the trial court's summary judgment in regards to four of the above mentioned causes of action: wrongful termination, invasion of privacy, negligent infliction of emotional distress and loss of consortium.[112]

First, the court held that the employer's access to back-up computer files did not constitute an unlawful interception under the state wiretap laws.[113] Second, the court dismissed the intentional infliction of emo-

---

A Pillsbury senior executive refuted Smyth's claim that Pillsbury assured its employees of privacy on the Pillsbury computer system. *See Letters to Fortune*, FORTUNE, Mar. 17, 1997, at 21-22. DeOcejo asserted that the district court's opinion relied solely upon Smyth's contentions when it stated that Pillsbury assured Smyth that his e-mail would remain private. *See id.* DeOcejo claimed that had the case gone to trial, Pillsbury would have offered a signed waiver that showed Smyth consented to e-mail monitoring. *Id.* This evidence would have shown that "Smyth acknowledged the company's right to review E-mail, and he signed the authorization well in advance of his difficulties with [Pillsbury]." *Id.* For a further discussion of the consent defense to e-mail privacy invasion, see *supra* notes 85-87 and accompanying text.

107. *See Pillsbury*, 914 F. Supp. at 101. The court determined that Pillsbury'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." *Id.* In addition, under the second reason for dismissal, the court once again noted that Pillsbury did not force the plaintiff to disclose personal information or invade the plaintiff's person, as would be the case with urinalysis or a personal property search. *See id.*

108. *See id.*

109. No. 95-2125 (Mass. App. Ct. 1996), *reprinted in The Week's Opinions; Superior Court, Massachusetts Lawyers Weekly*, Dec. 16, 1996, at 16.

110. *Id.* The employees' stored e-mail messages included messages containing nicknames for the employer and messages detailing the employer's extramarital affair with another employee. *See id.*

111. *See id.* One of the plaintiffs' spouses joined the suit as a co-plaintiff for the loss of consortium claim. *See id.*

112. *See id.* The court held that the employer was entitled to summary judgment on the claims under the state wiretap statute— intentional infliction of emotional distress and tortious interference with contractual relations. *See id.*

113. *See id.* The Massachusetts statute included a business exception to interception laws which stated that "'[i]t shall not be a violation of this section . . . for persons to possess an office intercommunication system which is used in the ordi-

tional distress claim because the employees did not meet their burden of proving extreme and outrageous conduct by the employer or severe emotional distress.[114] Third, the court allowed the continuance of the negligent infliction of emotional distress claim because the employees met their initial burden of alleging emotional distress resulting in physical harm.[115] Fourth, the court dismissed the employees' tortious interference with contractual relations claim because they did not allege an actual or prospective third-party contract.[116] Fifth, the court held that summary judgment was not appropriate for the invasion of privacy claim because two genuine issues of material fact remained: whether the employees had a reasonable expectation of privacy in their e-mail messages and whether the employer's actions were "an unreasonable, substantial or serious interference with [their] privacy."[117] Sixth, the court similarly held that summary judgment was not appropriate for the wrongful discharge claim because genuine issues of material fact existed for the invasion of privacy issues.[118] Finally, the court held that an employee's spouse had sufficient facts set forth in the complaint to allege a loss of consortium claim.[119]

At first, the *Restuccia* decision appears to be a pro-employee decision. The court, however, was only deciding whether summary judgment was proper in light of the allegations of the complaint.[120] Nevertheless, the plaintiff still faces serious obstacles at the trial level.

---

nary course of their business or to use such office intercommunication system in their ordinary course of their business.'" MASS. GEN. LAWS. Ch. 272, § 99 (1997). The court held that reading files that the system automatically backed up was a protected interception under the ordinary course of business exception. *See id.*

114. *See* No. 95-2125 (Mass. App. Ct. 1996), *reprinted in The Week's Opinions; Superior Court, Massachusetts Lawyers Weekly*, Dec. 16, 1996, at 16. The court stated that the plaintiffs' burden was to show that the "defendants intentionally caused severe emotional distress through conduct that was extreme and outrageous." *Id.*

115. *See id.* The court stated that such harm "must be manifested by objective symptomatology and substantiated by expert medical testimony." *Id.* One plaintiff claimed that she experienced sleeplessness, stomach aches and headaches and suffered a miscarriage. *See id.* The other plaintiff claimed that he experienced sleeplessness, gastrointestinal difficulties and fatigue as a result of the employer's actions. *See id.*

116. *See id.* The court stated that "[t]o succeed on a claim of interference with contractual relations, plaintiffs must prove that they had a contract with a third party, that the defendant knowingly and improperly induced the third party to break that contract and that plaintiffs were harmed by defendants' actions." *Id.*

117. *Id.* The court stated that under Massachusetts law, "a person shall have a right against unreasonable, substantial, or serious interference with his privacy." *Id.*

118. *See id.* The court stated that an employer may not discharge an at-will employee if the employer's reason violates a "clearly defined and well established public policy." *Id.* The employees based the wrongful discharge claim on the notion that an invasion of privacy is contrary to a "clearly defined and well established public policy." *Id.*

119. *See id.* Under Massachusetts common law, a spouse may recover "damages arising from personal injury of the other spouse caused by the negligence of a third person." *Id.*

120. *See id.*

## V. E-MAIL POLICIES IN THE WORKPLACE

Current law does not vest a strong privacy interest in an employee for e-mail in the workplace.[121] An employer, however, may provide employees with advance knowledge of how e-mail will be treated in their employment context by creating an e-mail monitoring policy.[122] Such a policy should clearly communicate to employees the employer's intentions regarding workplace privacy.[123] Furthermore, a well-disseminated e-mail policy could be an effective method to avoid invasion of privacy claims or complaints by employees.[124] Currently, it is estimated that only one-third of U.S. businesses utilizing e-mail systems have e-mail policies.[125] E-mail monitoring policies serve multiple purposes. They create clear standards to prevent employment disputes and insure consistent supervisory administration of employment relations.[126] As one commentator noted: "[M]ost importantly, they can make employees feel that the company subscribes to a philosophy of fairness and equal treatment in employment matters."[127] In addition, an e-mail monitoring policy will provide proof to the em-

121. *See* Hash & Ibrahim, *supra* note 68, at 909 ("It appears that current federal law, as well as state statutory and common law, favors employers when it comes to E-mail monitoring in the workplace."); Van Doren, *supra* note 19, at 12 ("Security measures such as assigning personal identification codes to employees and secret passwords to access specific networks reinforce the employees' belief that e-mail messages belong solely to the sender and the parties to whom the messages are sent."). For a further discussion of an employee's lack of privacy interest in workplace e-mail, see *supra* notes 35-93 and accompanying text.

122. *See* Glassberg et al., *supra* note 15, at 75 ("Employees can and will use E-mail for idle chitchat, gossip, and privileged or derogatory conversation when there is no policy suggesting its appropriate use.").

123. *See* Lee, *supra* note 68, at 469 (noting need to communicate company's expectations).

124. *See* Lorek, *supra* note 19, at 4G ("It's important for employers to have e-mail policies in place to prevent potential litigation."); Van Doren, *supra* note 19, at 12 ("[E]mployers can both avoid potential legal problems and ensure their right to monitor e-mail messages by implementing and communicating e-mail monitoring policies to their employees."); *see also* PERRITT, *supra* note 45, at 220 ("As a general matter, an employee can consent to conduct that would constitute an invasion of privacy absent the consent."). *See generally Employers Stepping Up*, *supra* note 28 (quoting Hal Coxson, management lawyer, as stating "I think employers should be up front with their employees about monitoring in the workplace. I think companies should have very explicit written policies that employees are aware of which inform them that they will be subject to monitoring for legitimate business purposes.").

125. *See* Brown, *supra* note 30, at 66. One group of commentators have suggested that an effective e-mail policy must "[b]e consistent with the policies regarding other communication media," "[c]onsider the rights and expectations of employees," "[e]ndeavor to protect employers' rights," "[b]e drafted by a cross-functional team composed of management, informations systems, legal, and human resource personnel" and "[b]e written and well communicated throughout the organization." Glassberg et al., *supra* note 15, at 74 fig.2.

126. *See* CHARLES G. BAKALY, JR. & JOEL M. GROSSMAN, THE MODERN LAW OF EMPLOYMENT RELATIONSHIPS 48 (2d ed. 1990) (noting that policies make employees feel that there is sense of fairness within company).

127. *Id.*

ployee, or to a court in the event of litigation, that the employer seeks to protect company property and resources, and does not seek to invade the employee's privacy rights.[128]

Prior to adopting an e-mail monitoring policy or manual, an employer should decide how binding they want their policy statement to be.[129] A majority of courts currently hold that an employer is contractually bound by the terms of employment manuals and policies.[130] These courts hold that unilateral contacts are formed between the employer and employee: the offer is the policy statement and the employee accepts by starting or continuing to work for the employer.[131] The argument for contractual validity is further strengthened because the employer voluntarily issues such policies.[132] A minority of courts, however, hold that policies or manuals are merely "unilateral expressions which can be followed or not at the employer's discretion."[133]

To avoid a dispute as to whether the policy or manual is binding, the employer should "clearly and prominently" state that the policy or manual does not grant the employee contractual rights.[134] Additionally, for monitoring consent purposes, the employer should adhere strictly to monitoring detailed in the e-mail monitoring policy.[135] One commentator has

128. *See* Gantt, *supra* note 66, at 358 ("[T]he policies serve as evidence . . . [of the company's] desire to protect its property.").

129. *See* BAKALY & GROSSMAN, *supra* note 126, at 57 (stating that intent of parties, as evidenced through language used, is often controlling).

130. *See id.* at 48.

131. *See id.* at 50.

132. *See id.* at 51 (noting that employer has no obligation to issue such policy). One state court has moved away from the strict application of contract offer and acceptance and held that an employer may unilaterally amend the policy without notice to the employee. *See* Toussaint v. Blue Cross & Blue Shield, 292 N.W.2d 880, 892 (Mich. 1980). Commentators have stated that the Michigan court upheld the continued validity of the policy "even if there is no evidence that the parties reached any agreement regarding the policy." BAKALY & GROSSMAN, *supra* note 126, at 51.

133. BAKALY & GROSSMAN, *supra* note 126, at 48. For a further discussion of the rationale of the courts holding manuals and policies to be unilateral expression by the employer, see *id.* at 52-54. In addition, a few courts have not directly decided whether an employer's policy or manual is contractually binding. *See id.* at 48.

134. *See id.* at 57 ("[A]n employer should . . . assume that any procedures or guidelines adopted as a matter of 'policy' will be enforced against it unless it clearly and prominently states that its policies do not grant the employee any contractual rights."). Courts are likely to nullify such a "disclaimer" if the employer acts in a manner inconsistent with the terms of the policy or manual, even if the disclaimer is otherwise sufficiently clear to be given effect. *See id.* at 60.

135. *See* Baumhart, *supra* note 41, at 934 ("[A]n employer who intends to obtain employee consent by announcing a monitoring policy must be careful to operate within the confines of the policy."); Gantt, *supra* note 66, at 356 (discussing preeminent consent defense case, Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983), which held that "employee consent will be carefully limited to the confines of an employer monitoring policy"). For a further discussion of employee consent to e-mail monitoring, see *supra* notes 85-87 and accompanying text. In

suggested that if an employer prefers engaging in extensive monitoring of employee e-mail, he or she should "expand the permissible scope [of monitoring] by offering legitimate interests justifying broad monitoring policies."[136]

In addition to explaining that e-mail is to facilitate business communications, an e-mail monitoring policy should include three main provisions: the employer's right to access e-mail provision, the personal use provision and the forbidden content provision.[137] First, the employer's right to access provision should state that the employer reserves the right to access any of the employees' e-mail messages transmitted on the employer's system.[138] Second, the personal use provision should inform the employee to what extent the company's e-mail system may be used for personal use,

---

*Watkins*, the employer's monitoring policy for telephone calls allowed the employer to monitor business-related conversation and to monitor personal telephone conversations to the extent necessary to determine whether the call was for business or personal purposes. *Watkins*, 704 F.2d at 579. In regards to the employer monitoring an entire personal conversation of an employee, the United States Court of Appeals for the Eleventh Circuit held that the employer's policy limited the employee's consent for full conversation monitoring to only business-related calls, and the full conversation monitoring of a personal conversation violated 18 U.S.C. § 2511. *See id.* at 581-82.

136. Gantt, *supra* note 66, at 358.

137. *See A Sample E-Mail Policy*, CONN. L. TRIB., Dec. 18, 1995, at 12 (discussing sample e-mail policy developed by labor, employment and employee benefits group).

138. *See id.* The following is an excerpt from a sample e-mail policy drafted by Margaret Hart Edwards, an attorney from the San Francisco- and Sacramento-based law firm of Landels, Riley & Diamond:

> Management's Right to Access Information
>
> The electronic mail system has been installed by XYZ to facilitate business communications. Although such employee has an individual password to access this system, it belongs to the Company and the contents of e-mail communications are accessible at all times by XYZ management for any business purpose. These systems may be subject to periodic unannounced inspections, and should be treated like other shared filing systems. All system passwords and encryption keys must be available to Company management, and you may not use passwords that are unknown to your supervisor or install encryption programs without turning over encryption keys to your supervisor.
>
> All e-mail messages are Company records. The contents of e-mail properly obtained for legitimate business purposes, may be disclosed within the Company without your permission. Therefore, you should not assume that messages are confidential. Back-up copies of e-mail may be maintained and referenced for business and legal reasons.

*Id.*; *see also* Phillip Rosen & Margaret Bryant, *Draft a Policy Before You Monitor Email*, HR REP., June 1996, at 3 (suggesting that e-mail monitoring policies should include provision stating "[e]-mail may be monitored for legitimate purposes without prior notice to protect confidential information, prevent theft or abuse of the system, or monitor work flow and productivity"). Such a provision could also include information dealing with "how often the system is monitored, by whom and specify the purpose of the monitoring." Mattson, *supra* note 18, at 16.

if personal use is to be allowed at all.[139] If, however, an employer allows personal use e-mail, he or she should be careful to not discriminatorily prohibit certain types of employee e-mail, such as prohibiting pro-union messages.[140] Third, the forbidden content provision should inform the employee that certain types of e-mail content are strictly forbidden, such as sexually explicit or racially offensive messages.[141] By including the

139. *See A Sample E-Mail Policy, supra* note 137, at 12. The following is the personal use provision of Ms. Edwards' sample e-mail policy:

> Personal Use of E-Mail
>
> Because XYZ provides the electronic mail system to assist you in the performance of your job, you should use it for official Company business. Incidental and occasional personal use of e-mail is permitted by XYZ, but these messages will be treated the same as other messages. XYZ reserves the right to access and disclose as necessary all messages sent over its e-mail system, without regard to content.
>
> Since your personal messages can be accessed by XYZ management without prior notice, you should not use e-mail to transmit any messages you would not want read by a third party. For example, you should not use the XYZ e-mail for gossip, including personal information about yourself or others, for forwarding messages under circumstances likely to embarrass the sender, or for emotional responses to business correspondence or work situations. In any event, you should not use these systems for such purposes as soliciting or proselytizing for commercial ventures, religious or personal causes or outside organizations or other similar, non-job-related solicitations. If XYZ discovers that you are misusing the e-mail system, you will be subject to disciplinary action up to and including termination.

*Id.*

140. *See* E.I. du Pont de Nemours & Co., 311 N.L.R.B. 893 (1993). E.I. du Pont de Nemours & Co. ("DuPont") allowed its employees to distribute personal e-mail communications over its computer system. *See id.* at 919. In light of DuPont's then existing policy, an administrative law judge from the National Labor Relations Board ruled that DuPont could not prevent union employees from distributing union information in e-mail communications. *See id.* One commentator noted: "Although . . . whether unions have the right to use E-mail systems is still unsettled, the . . . lesson from DuPont is clear. *If a corporation knowingly allows its employees to use E-mail for personal purposes, the company will be hard pressed to justify a ban on pro-union messages.*" Morris et al., *supra* note 42, at 345 (emphasis added).

141. *See A Sample E-Mail Policy, supra* note 137, at 12. The following is the forbidden content provision of Ms. Edwards' sample e-mail policy:

> Forbidden Content of E-Mail Communications
>
> You may not use XYZ's e-mail system in any way that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale. Examples of forbidden transmissions include sexually-explicit messages, cartoons, or jokes; unwelcome propositions or love letters; ethnic or racial slurs; or any other message that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs.
>
> Use of the Company-provided e-mail system in violation of this guideline will result in disciplinary action, up to and including termination.

*Id.* Furthermore, one commentator has suggested that at a minimum, all e-mail policies should forbid the following types of messages: "racial or ethnic slurs," "sexual harassment," "distribution of corporate trade secrets" and "distribution of third-party copyrighted materials." Wasch, *supra* note 7, at 13. Furthermore, Patri-

above provisions in an e-mail monitoring policy, the employer lowers the employee's expectations of privacy in workplace e-mail communications and weakens the employee's privacy invasion allegations.[142]

One of the most important steps in instituting an effective e-mail policy in a workplace is informing the employees as to its content.[143] When an employer adequately disseminates the contents of an e-mail policy, he or she has a greater level of protection in the event of litigation because

---

cia L. Morris, the Dean of the School of Education and Urban Studies at Morgan State University, suggests that it is important to caution same-race, same-ethnic, or same-gender employees from sending e-mail "jokes" pertaining to their own race, ethnicity or gender because such jokes "reinforce stereotypes." Singletary, *supra* note 24, at A1. For a discussion of the Morgan Stanley and Citibank lawsuits involving racially offensive e-mail messages, see *supra* notes 22-24 and accompanying text.

In addition, Ms. Edwards included a provision within her sample e-mail policy discussing e-mail encryption, entitled "Password and Encryption Key Security and Integrity," which stated: "Employees are prohibited from the unauthorized use of passwords and encryption keys of other employees to gain access to the other employee's e-mail messages." *A Sample E-Mail Policy, supra* note 137, at 12.

142. *See* Daniel W. McDonald et al., *Intellectual Property and Privacy Issues on the Internet,* 79 J. PAT. & TRADEMARK OFF. SOC'Y 31, 56 (1997) (advising that employers "take precautionary steps" monitoring employee e-mail communications because "there is little case law . . . to provide definitive guidance as to liability"). One commentator has suggested the benefits of an e-mail monitoring policy that lowers the employee's expectation of privacy:

> An employer should develop a policy that effectively lowers the expectation of privacy in advance, present it to the employees in writing and through training programs including, if possible, actual demonstrations. This will greatly improve an employer's chances of tipping the privacy balance in its favor in future litigation challenging the surveillance or monitoring. The lower the expectation of privacy on the part of the employee, the greater the likelihood that searches and monitoring will be held valid. The bottom line is that the employer should do everything it reasonably can, consistent with its culture and employee morale, to lower the privacy expectations of employees.

Lee, *supra* note 68, at 470.

143. *See* Emily Leinfuss, *Policy over Policing; It's Easy to Develop E-Mail and Internet Policies, but Education and Documentation Are Crucial to Their Success,* INFOWORLD, Aug. 19, 1996, at 55 ("Companies have a responsibility to post policies. They should be embedded in written documentation and 'advertised' in a banner on company systems.") (quoting Richard Power). Some suggested methods for employers to communicate e-mail policies to employees include providing all new employees with a written version of the policy, having an informational message appear each time an employee logs on to the company system, seeking acknowledgment through signature forms and providing notification to employees when the employee receives new computer hardware or software. *See* Van Doren, *supra* note 19, at 12; *see also* Rosen & Bryant, *supra* note 138, at 3 ("Program a notice repeating . . . the policy. Install it to appear on the computer screen whenever someone logs on to the email system."); Leinfuss, *supra,* at 55 (stating that some employers recommunicate e-mail policies in company's bimonthly newsletters). For example, the Minneapolis office of Deloitte & Touche provides employees with a written e-mail policy and it requires employees to sign an acknowledgment form which states "that they have read the policy and consent to having [their] communication monitored." Mattson, *supra* note 18, at 16.

the employee cannot claim they were unaware of the employer's policy.[144] The employee's awareness of the monitoring also satisfies the consent requirements under the Stored Communications Act, thereby protecting the employer from potential liability.[145] In addition, employees are more likely to believe that e-mail monitoring is an acceptable practice if they are informed about the employer's policy.[146] Along with creating and communicating the e-mail policy, the employer should also explain to the employee the dangers associated with e-mail communications in the workplace.[147] For example, the employer should explain to its employees the effects of an e-mail message on the litigation process.[148]

## VI. CONCLUSION

Generally, employees in the private sector should expect little, if no, legal privacy interest in the e-mail that they send or receive from workplace computers.[149] Under current federal statutory enactments and state common law, an employer has a right to monitor and access employee e-mail sent and received from company computer systems.[150] A member of the United States Senate has unsuccessfully sought to require employers to notify employees if the employer intends to monitor workplace e-mail

144. *See* Van Doren, *supra* note 19, at 12 ("Making sure that the e-mail policy is clearly communicated to employees provides a level of protection from those employees who seek legal recourse claiming they were unaware of the practice.").

145. *See* Mattson, *supra* note 18, at 16 ("One of the biggest ways that employers are protecting themselves [from federal and state wiretap laws] is by obtaining . . . consent through publication of written e-mail policies."). For a further discussion of the consent defense under federal law, see *supra* notes 85-87 and accompanying text.

146. *See* Van Doren, *supra* note 19, at 12 (reporting that 1993 study found that "a significantly higher amount of [employee e-mail users] believed that monitoring workplace e-mail was acceptable when the employer had initially informed them about the monitoring policy").

147. *See* Parry Aftab, *A Carefully Planned E-mail Policy is the Best Defense in a Litigation*, N.Y. L.J., July 2, 1996, at 5. An employer should explain to employees two important points: first, that erased or deleted e-mail may "linger forever in backup tapes and stored printouts" and second, that their more relaxed e-mail communications can "lead to misunderstandings and unwarranted liability." *Id.* Mr. Aftab suggests that employers should also tell their employees that nothing should appear in an e-mail message if it should not appear in a memorandum or a letter. *See id.*

148. *See* Michael F. Cavanaugh, *E-mail Privacy: A Glass Almost Half-Full*, COMPUTERWORLD, Mar. 18, 1996, at 37. A recent survey conducted by the Society for Human Resource Management found that only 30% of employers surveyed had explained to their employees that e-mail messages can be discoverable materials during the discovery phase of judicial actions. *See id.*

149. For a further discussion of an employee's lack of privacy interest in workplace e-mail, see *supra* notes 35-93 and accompanying text.

150. For a further discussion of current federal statutory enactments and state common law that allow access to employee e-mail accounts, see *supra* notes 45-93 and accompanying text.

communications.[151] In addition, several state legislatures have debated whether employers should notify employees of monitoring activity, yet no pro-employee privacy statute has been enacted.[152]

In order to promote and maintain a desirable workplace environment, employers should seek to create an acceptable balance between the need to monitor workplace e-mail communications and the legitimate privacy concerns of its employees.[153] One commentator suggests that employers should only monitor employee e-mail for administrative necessity or to protect some justifiable legal interest.[154] Furthermore, employment attorneys are now recommending to their clients that they should limit workplace e-mail monitoring.[155] As e-mail use continues to increase, employers should adopt a formal, well-publicized e-mail policy to ensure employees are aware of their privacy rights in the private-sector workplace.[156] As the influential Warren and Brandeis article proclaimed in 1890, "the next step . . . must be taken [to secure] . . . the individual . . . the right 'to

---

151. *See* Andrea Bernstein, *Who's Reading Your E-Mail*, NEWSDAY, July 15, 1996, at A21. Senator Paul Simon introduced legislation to the United States Senate that would increase employee rights by requiring an employer to notify employees about electronic monitoring and to communicate to employees how the information would be used. *See id.* Although the Senate has never voted on the proposed legislation, Senator Simon warned that "rapid advances in office electronic technology may be outstripping personal privacy rights." *Id.*

152. *See* Halloran, *supra* note 27, at A1. The state legislatures in Washington and Wisconsin failed to enact proposed legislation that would have limited an employer's access to e-mail. *See id.* The Arkansas state legislature failed to enact proposed legislation in 1995 that would have required employers to notify employees of all personal surveillance of computer e-mail, in addition to camera surveillance and taping or listening to telephone conversations, that would have occurred in the workplace. *See* H.B. 2017, 80th Reg. Sess. (Ark. 1995), *summary available in* WESTLAW, BILLS-OLD File. In addition, the Colorado state legislature was recently debating the employer monitoring notification requirements. *See* Halloran, *supra* note 27, at A1.

153. *See* Peter Danzinger, *E-mail Monitoring Can Hurt Morale*, THE TIMES UNION (Albany), Mar. 22, 1997, at D10 (advising that "[m]onitoring can have negative effects on employees and company morale").

154. *See* Baumhart, *supra* note 41, at 947 ("Additionally, employers should review employee E-mail only when administratively essential. . . . [and] should confine its review to transactional data whenever possible . . . .").

155. *See* Alan Stern, *Electronic Mail Raises Thorny Legal Questions*, THE DENVER POST, Apr. 8, 1996, at C-12 ("[E]mployment lawyers are advising their clients to monitor their employees' e-mail only for legitimate business purposes . . . ."). In addition, one commentator reported that employment attorneys believe that employers should seek advance consent from employees before commencing e-mail monitoring. *See id.*; *see also* Baumhart, *supra* note 41, at 948 ("[T]he cautious employer should confine its review to transactional data whenever possible, reading message content only when a narrower search will not accomplish its legitimate or substantial business purpose.").

156. For a further discussion of the suggested elements of an e-mail monitoring policy and the positive impact of adopting such a policy for private-sector workplaces, see *supra* notes 121-48 and accompanying text.

be let alone.'"[157] Private-sector employers have begun to address this important issue and take the "next step"; recent research efforts have concluded that most American companies using e-mail systems in their workplace are in the process of adopting formal e-mail policies.[158]

*Kevin J. Baum*

157. Warren & Brandeis, *supra* note 1, at 195. For a further discussion of the Warren and Brandeis article, see *supra* notes 1-6 and accompanying text.

158. *See* Houlder, *supra* note 16, at 14 (reporting that e-mail policies "usually cover legal and security matters, together with guidelines about message style and the frequency with which messages should be sent"). For a further general discussion of private-sector e-mail monitoring policies, see *supra* notes 121-48 and accompanying text.