ELECTRONIC COMMUNICATIONS IN THE WORKPLACE: E-MAIL MONITORING AND THE RIGHT OF PRIVACY

Kevin P. Kopp

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."[1]

I. INTRODUCTION

The foregoing excerpt, uttered more than a century ago, accurately depicts the state of the law of privacy in today's computer age. The thesis is timeless and rests on the fundamental notion that as society progresses and evolves, so too must the law. The impetus behind the above proclamation was the advent of new technologies such as instantaneous photographs and recording devices which were being used with increasing frequency by the mass media.[2] It is axiomatic that today's computer technology presents an even greater threat to privacy.

Computer technology has revolutionized modern communications with the advent of electronic communications, specifically e-mail.[3] The impact of e-

---

[1]Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890). Commentators have credited the Warren and Brandeis article as the legal birth of the modern right of privacy. *See* Kevin J. Baum, Comment, *E-mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1042 n.1 (1997). The article has been hailed as having "had as much impact on the development of law as any single publication in legal periodicals." *Id.* (citing RICHARD C. TURKINGTON *ET AL.*, PRIVACY: CASES AND MATERIALS 31 (1992)).

[2]*See* Warren and Brandeis, *supra* note 1, at 195; *see also* Baum, *supra* note 1, at 1042 n.3.

[3]The term "e-mail" is short for "electronic mail." In discussions leading to the enactment of the Electronic Communications Privacy Act of 1986, the Senate Report described e-mail as a technology that enables two parties to communicate through the transmission of a digital message over public or private telephone lines. *See* S. Rep. No. 99-541, 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555. The e-mail message is held in a

mail has been particularly significant in the workplace. It has been estimated that ninety-percent of large companies, sixty-four percent of mid-size companies and forty-two percent of small companies currently utilize e-mail systems.[4] A recent poll revealed that over forty million employees correspond via e-mail and the number is estimated to increase by twenty percent every year.[5] These statistics are indicative of the popularity of electronic communication in today's workplace.[6] E-mail technology has facilitated more efficient inter-office communication, as well as extra-office communication with clients, customers and other business and personal associations.[7] In many instances, e-mail has effectively replaced the hand or type-written note, letter or memorandum.[8]

The benefits of e-mail in the workplace, coupled with its growing and already pervasive use, are compromised by the tendency of employers to monitor the e-mail messages of its employees.[9] In fact, a recent study found that thirty-two percent of employers who maintain e-mail systems routinely engage in random monitoring of their employees' e-mail communications.[10] In an even

---

computer 'mail box' until it is retrieved by the recipient. *See id.* See Part II, Section B of this Comment for a complete discussion of the Electronic Communications Privacy Act.

[4]*See* Mark S. Dichter and Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, Seminar Before The American Employment Law Council, Fourth Annual Conference (Oct. 2-5, 1996) (outline available at <http://www.mlb.com/speech1.htm>, (last visited 04/18/97) (citing a recent survey conducted by the Gallup Organization).

[5]*See id.*

[6]*See* Steven Miller, *E-mail's Popularity Poses Workplace Privacy Problems*, BUS. FIRST OF COLUMBUS, Oct. 3, 1997 ("Electronic mail messages are fast becoming the communications vehicle of choice for much of corporate America.").

[7]*See* C. Forbes Sargent, III, *Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues*, 41 BOSTON B.J. 6 (May/June 1997) (noting the growing use and popularity of e-mail in the workplace).

[8]*See id.*

[9]*See* Baum, *supra* note 1, at 1016.

[10]*See id.* (citing Liz Halloran, *Big Brother Is Reading This; Your Boss Can Browse Your E-mail*, HARTFORD COURANT, April 15, 1996, at A1). The study was conducted by The Society for Human Resource Management. *See id.* Its statistics were derived from a poll of 538 business executives. *See id.* It should be noted that the nature of e-mail makes it particularly susceptible to monitoring. For example, all e-mail transmissions in the workplace that occur over company-owned networks must pass through a central routing computer. *See* Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the*

more troubling study, the American Management Association found that of the employers who maintain monitoring and surveillance policies, nearly one quarter do not inform their employees of potential monitoring.[11] Thus, many employees mistakenly assume that their e-mail communications are private.[12]

To examine the legal implications of e-mail monitoring in the workplace, it is first necessary to consider the circumstances that motivate employers to monitor employees. One possible motivation could be the ease with which an employer may conduct monitoring.[13] Yet another, more legitimate purpose could be to curb employee misuses or abuses of an employer-provided e-mail system.[14] Such abuses could take the form of wasted time spent sending personal messages to friends, family or co-workers during business hours.[15] More

---

Private Sector Workplace, 8 HARV. J.L. & TECH. 345, 349 (Spring 1995). This central computer automatically stores all e-mail transmissions which may then be easily accessed by the service provider, network administrator or the employer itself. *See id.* at 349-50; *see also* Sargent, *supra* note 4, at 6. Furthermore, new software programs have been developed to assist employers in monitoring large volumes of e-mail. *See* Amitai Etzioni, *Some Privacy, Please, For E-mail*, CHI. DAILY L. BULL., Nov. 24, 1997 at 6. These programs are designed to automatically detect key words that allude to the type of behavior or communication the company wishes to control or prohibit. *See id.* After scanning all of the messages in the e-mail system, only those messages that contain these key words are retrieved for the employer to peruse. *See id.*

[11]*See* 5 Telecom & Network Sec. Rev., No. 6 (June 1, 1997). The survey consisted of over 900 American Management Association member companies. *See id.*

[12]*See* Sargent, *supra* note 7, at 6 ("Since an employee typically uses a password to log onto the office computer system, and because electronic mail is sent only to its designated recipient who usually must access his or her personal 'mailbox' by means of a password, the common assumption is that e-mail is as private and confidential as communication via the U.S. Postal Service."). Another common assumption is that once an e-mail message is deleted it no longer exists. *See id.* Thus, it should also be noted that after a recipient deletes an e-mail message, that same message may still be stored in the e-mail system. *See id.* As such, the deleted message remains accessible to the employer, unbeknownst to either the sender or recipient of that message. *See id.*

[13]*See* Gantt, *supra* note 10, at 349; *see also* Anne L. Lehman, *E-mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMMLAW CONSPECTUS 99 (1997). The ease with which employees may be monitored enhances the incentive of employers to conduct the monitoring. *See* Lehman, at 99. As between monitoring and not monitoring, an employer is likely to choose the former in light of potential liability issues involving the contents of employee e-mail. *See id.*

[14]*See* Jarrod J. White, *E-mail@Work.Com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1079-80 (1997); *see also* Etzioni, *supra* note 10, at 6.

[15] *See* White, *supra* note 14, at 1080; *see also* Len Lewis, *Big Brother is Watching,*

serious abuses could involve sending harassing messages to co-workers,[16] or revealing trade secrets to rival companies.[17]

While the circumstances motivating employers to monitor e-mail may seem compelling, there are far less invasive tactics that may be implemented to effectively curb employee abuse of e-mail. A written e-mail policy that clearly defines appropriate and inappropriate uses of the e-mail system is primary among them.[18] In addition to defining proper limits, a written e-mail policy may also serve to inform employees of potential monitoring, thereby reducing or eliminating any expectation of privacy employees may have regarding their e-mail.[19] On the other hand, the most effective policy regarding e-mail monitoring may be one that is more protective of employee privacy.[20] Policies or practices of employers that endorse invasive monitoring create an adversarial relationship between employer and employee.[21] In fact, studies have shown that efficiency and productivity levels are at their highest in workplaces that recognize and respect employee privacy.[22]

(Employees Privacy Rights and the Internet), PROGRESSIVE GROCER, Feb. 1, 1997 (noting that as much as "25 percent of employees' time can be spent on e-mail").

[16]*See id.* ("[S]tudies indicate that over twenty percent of E-mail users have received sexually harassing E-mail.").

[17]*See* Etzioni, *supra* note 10. E-mail makes it possible for employees to easily disseminate trade secrets or proprietary information to outside parties, or to co-workers who may not otherwise be privy to such information. *See* Frank C. Morris, Jr., *Issues from the Electronic Workplace E-mail Communications: The Developing Employment Law Nightmare*, SB07 ALI-ABA 335, 338 (July 25, 1996).

[18]*See* Sargent, *supra* note 7, at 20; *see also* Baum *supra* note 1, at 1037-38 (noting the need for an e-mail policy to include a personal use provision informing the employee of the extent to which the e-mail system may be used for personal use). See note 206 *infra* for a sample e-mail policy.

[19]*See* White, *supra* note 14, at 1103 (explaining that an employee's acceptance of the terms of the e-mail policy would be tantamount to consent to the monitoring).

[20]*See* Gantt, *supra* note 10, at 419-24 (arguing that business interests are better served in an environment where personal privacy is protected).

[21]*See id.* at 421 ("Business experts . . . argue that successful companies do not treat their employees like enemies but rather offer employees a participatory environment in which they develop personal and professional incentives to work efficiently.").

[22]*See id.* at 421-22 ("Promoting an atmosphere that fosters trust promotes cooperation and teamwork, which further increase employee productivity . . . In sum, employees who have a distinct area of workplace privacy may work more efficiently than employees who

This Comment will explore the issue of whether and to what extent existing law protects employees' right to privacy. Part II will examine the applicability of federal and state constitutional provisions to e-mail privacy in the workplace. Part II will examine the impact of federal and state statutory enactments. Part II will also explore the various common law tort causes of action that may be available to aggrieved employees. Finally, Part III will assess the current state of the law with regard to e-mail privacy in the workplace, and demonstrate the inadequacy of this law in protecting employee privacy. In this process, recent cases involving e-mail privacy will be analyzed. This Comment will highlight the current trend toward unrestricted monitoring by employers and argue for greater protection for e-mail privacy in the workplace.

II. EXISTING LAW AND ITS APPLICABILITY TO ELECTRONIC COMMUNICATIONS IN THE WORKPLACE

A. CONSTITUTIONAL LAW

The Fourth Amendment to the United States Constitution provides in pertinent part, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[23] Although not explicitly mentioned in the United States Constitution, the general right of privacy is rooted in the Fourth Amendment.[24] The United States Supreme Court has explicitly endorsed the right of privacy pursuant to the Fourth Amendment in cases such as *Griswold v. Connecticut*[25] and *Katz v. United States*.[26] However, the Fourth Amendment applies only to governmental actors.[27] Thus, the Fourth Amendment protects public employ-

---

are continuously being scrutinized by their employers.").

[23]U.S. CONST. amend. IV.

[24]*See* Lehman, *supra* note 13, at 100. An in-depth examination of the general right of privacy is beyond the scope of this Comment. For a more extensive discussion see Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (1992) (examining the evolution of privacy law from the Warren and Brandeis article to the present).

[25]381 U.S. 479 (1965) (holding unconstitutional a statute banning the use of contraceptives on the basis that the Bill of Rights, including the Fourth Amendment, created a zone of privacy to be protected against governmental intrusion).

[26]389 U.S. 347 (1967) (holding that warrantless electronic surveillance violated the Fourth Amendment which protects privacy against unreasonable searches and seizures).

[27]*See* Thomas R. Greenberg, Comment, *E-mail and Voice Mail: Employee Privacy and*

ees in the public sector workplace, but does not extend to the private sector workplace to protect private employees.

The United States Supreme Court's landmark ruling in *O'Connor v. Ortega*[28] defines the extent to which the Fourth Amendment protects employee privacy in the public employment context. In *Ortega*, a psychiatrist charged state hospital officials with violating his Fourth Amendment rights after they searched his office and seized various items from his desk and file cabinets.[29] The Court held that the propriety of a workplace search, at its inception and in its scope, "should be judged by the standard of reasonableness under all the circumstances."[30] The Court concluded that under this standard, the Fourth Amendment is violated only if public employees have "an expectation of privacy that society is prepared to consider reasonable."[31] This standard requires balancing the employer's need for control and supervision of the workplace against the privacy interests of employees.[32]

Although the Fourth Amendment offers limited protection to public employees,[33] it does not protect private employees from workplace searches conducted by their employers.[34] Thus, even if society is prepared to recognize the reasonableness of private employees' privacy expectations, the Fourth Amendment to the United States Constitution affords no protection in the private sector

---

the Federal Wiretap Statute, 44 AM. U. L. REV. 219, 220 (1994).

[28]480 U.S. 709 (1987). For an in-depth analysis of *Ortega* and its progeny, as well as public employee privacy, *see generally* Gantt, *supra* note 10, at 380-86.

[29]*See* Ortega, 480 U.S. at 711.

[30]*Id.* at 725-26.

[31]*Id.* at 715 (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

[32]*See id.* at 719-20.

[33]*See* Steven B. Winters, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail*, 1 S. CAL. INTERDISCIPLINARY L.J. 85 (1992). Winters argues that "federal courts have so narrowly circumscribed the public employee's Fourth Amendment work-related privacy rights that these rights have all but vanished completely." *Id.* at 116.

[34]*See* Greenberg, *supra* note 27, at 220; Lehman, *supra* note 13, at 100-01; Baum, *supra* note 1, at 1018. The Fourth Amendment to the United States Constitution only limits governmental action. *See id.* Therefore, the Fourth Amendment only protects employees who are employed by federal, state or local governmental bodies. *See id.*

workplace.[35]

Unlike the Federal Constitution, many state constitutions explicitly guarantee a right of privacy akin to the protection provided by the Fourth Amendment's prohibition of unreasonable searches and seizures.[36] Like the Fourth Amendment, however, this protection generally extends only to public employees.[37] Therefore, even in those states that recognize and extend privacy rights under their state constitutions, private sector employees remain unprotected.[38]

To date, California is the only state that has extended its state constitutional privacy protection to private employees.[39] In an unpublished opinion, however, a California Superior Court declined to extend constitutional privacy protection to the e-mail communications of private employees.[40] In *Flanagan v. Epson America*, an employee of Epson brought a class action challenging Epson's routine monitoring of employee e-mail.[41] In rejecting the employee's

---

[35]*See id.*

[36]*See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); 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 . . ."); 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."); 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 . . ."); 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 be invaded, without authority of law.").

[37]*See* Baum, *supra* note 1, at 1019.

[38]*But see* Porten v. University of San Francisco, 134 Cal. Rptr. 839 (Cal. Ct. App. 1976) (holding that California's constitutional privacy rights extend to both public and private employees).

[39]*See Porten*, 134 Cal. Rptr. at 841-42.

[40]*See* Flanagan v. Epson America, No. BC007036 (Cal. Super. Ct. 1991), *discussed in* Baum, *supra* note 1, at 1019. See notes 72-75 *infra* for a further analysis of this case.

[41]*See id.*; *see also* Sargent, *supra* note 7, at 19 (discussing Flanagan v. Epson America, No. BC007036 (Cal. Super. Ct. 1991).

constitutional claim, the court reasoned that an extension of constitutional privacy rights to protect employee e-mail communications from employer monitoring should be undertaken by the legislature and not the judiciary.[42]

B. STATUTORY ENACTMENTS

In the absence of constitutional protection, employees are increasingly looking to Congress and their state legislatures for statutory protection.[43] In response to Congress' perception that abuses associated with new technologies pose a substantial risk to civil liberties, the Electronic Communications Privacy Act of 1986 ("ECPA")[44] was enacted.[45] The ECPA is "the only federal statute that specifically addresses the interception and accession of e-mail communications."[46] The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[47] which merely proscribed the unauthorized interception of wire and oral communications.[48] Essentially, the ECPA extends Title III's existing prohibitions to the unauthorized interception of electronic

---

[42]*See Flanagan*, No. BC007036, *discussed in* Baum, *supra* note 1, at 1019. The class action also alleged that Epson violated California's wire tap law, but the Court held that only telephone conversations were protected under the wire tap law. *See* Gantt, *supra* note 10, at 360 (discussing the *Flanagan* case).

[43]*See* Baum, *supra* note 1, at 1018.

[44]Pub. L. No 99-508, 100 Stat. 1848, as amended, 18 U.S.C. §§ 2510-22, 2701-10, 3117, 3121-26 (1994).

[45]*See* White, *supra* note 14, at 1080-81. The ECPA was enacted in response to a 1985 Office of Technology Assessment report "which emphatically expressed the threat of privacy posed by unregulated invasions into electronic communications." Gantt, *supra* note 10, at 425 n.45.

[46]Gantt, *supra* note 10, at 351. "Electronic communication," as defined by the ECPA, is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate commerce." 18 U.S.C. § 2510(12) (1994). Although not explicitly stated in this definition, the legislative history clearly evidences Congress' intent to include e-mail within the definition of "Electronic Communications." *See* Dichter and Burkhardt, *supra* note 4.

[47]*See* Pub. L. No. 90-351, 82 Stat. 197, 211-25, amended by 18 U.S.C. §§ 2510-21 (1994).

[48]*See* Gantt, *supra* note 10, at 351.

communications.[49] Thus, Title III and the ECPA together, prohibit the intentional or willful interception, accession, disclosure or use of one's wire, oral or electronic communication.[50]

The definition of "intercept" under the former Title III was limited to aural acquisition of a wire or oral communication.[51] Title I of the ECPA broadens this definition to include the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[52] This protection extends to cover the intentional interception of communications by unauthorized individuals, as well as governmental agents.[53] One commentator suggests that "[f]rom this emphasis on 'third party' interception, the ECPA does not explicitly offer protection from employers who access or intercept the electronic communications of their employees."[54] Instead, the ECPA appears to offer protection only from the unauthorized interception by outside parties or from another employee who has exceeded "his or her authority when accessing, intercepting, or disclosing information on a private corporate system."[55]

In addition to Title I's prohibition of the unauthorized interception of electronic transmissions, Title II of the ECPA ("Stored Communications Act")[56] provides protection against the unauthorized accession of electronic communications in storage.[57] Title II defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to

---

[49]*See id.*

[50]*See* 18 U.S.C. § 2511 et seq. (1994).

[51]*See* S. Rep. No. 541, 99th Cong., 2d Sess. 3 (1986). The Title III definition of "interception" "only applies where the contents of a communication can be overheard and understood by the human ear." *Id. See also* Greenberg, *supra* note 27, at n. 66. Data transmissions, such as e-mail, are non-aural communications.

[52]18 U.S.C. § 2511(1)(c) (1994).

[53]*See id.* at § 2511(1)(a), (2)(a)(ii)(A) (1994). Title I requires that governmental agents obtain a signed court order that instructs a service provider to assist the governmental agents in intercepting the communication. *See* 18 U.S.C. § 2516(1) (1994).

[54]Gantt, *supra* note 10, at 352.

[55]*Id.*

[56]18 U.S.C. §§ 2701-2711 (1994).

[57]*See id.*

the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[58] A violation of the Stored Communications Act occurs when a person "intentionally accesses without authorization a facility through which an electronic communication service is provided."[59]

The remedial framework of the ECPA provides for both civil and criminal penalties.[60] A civil plaintiff who successfully proves a violation of the ECPA is entitled to the greater of actual damages suffered and any profits made by the violator, or the greater of $100 a day for each day the Act was violated or $10,000.[61] The ECPA's remedial provisions also provide for the award of attorney's fees, costs and equitable relief.[62] Criminal sanctions under the ECPA include fines and/or up to five years imprisonment.[63]

Although none the provisions in the ECPA or its legislative history appear to limit its applicability to employer monitoring of employee e-mail communications, the ECPA contains three primary exceptions that may have the same

---

[58]*Id.* at § 2510(17) (1994).

[59]*Id.* at § 2701(a)(1) (1994).

[60]*See id.* at § 2520(a)-(b), 2511(4)(a) (1994).

[61]*See id.* at § 2520(c)(2). The provision reads in pertinent part:

> [T]he court may assess as damages whichever is the greater of —
>
> > (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or
> >
> > (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

Id. Punitive damages are available for a violation of the interception provisions, but are not available under the storage access provisions. *See id.* at § 2520(b)(2).

[62]*See id.* at § 2520(b)(3).

[63]*See id.* at § 2511(4)(a)-(b). The provision reads in pertinent part: "[W]hoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." *Id.* A first offense with no tortious or illegal purpose carries only a fine or imprisonment for "not more than one year, or both." *Id.* at Section 2511 (4)(b)(i).

practical effect.[64] These exceptions are known as the provider exception;[65] the ordinary course of business exception;[66] and, the consent exception.[67] Each of these exceptions will be discussed below in the context of e-mail monitoring in the private sector workplace.

1. PROVIDER EXCEPTION

The provider exception contained in the ECPA generally exempts e-mail service providers from the ECPA prohibitions on interception or accession of e-mail communications in the workplace.[68] The provider exception has been broadly interpreted by commentators who suggest that most private employers will be exempt from ECPA liability so long as the employer is the provider of the e-mail system.[69] This interpretation effectively reserves to employers an unrestricted right to monitor the e-mail communications of its employees on a company-owned e-mail system.[70] Other commentators, however, warn that the provider exception may not apply to employers who merely provide e-mail service to its employees through a common carrier, such as America Online, Compuserve, or Prodigy.[71]

---

[64]*See id.* at § 2511(2)(a)(i), 2510(5)(a), 2511(2)(d). *See also* Gantt, *supra* note 10, at 352.

[65]*See* 18 U.S.C. § 2511(2)(a)(i).

[66]*See id.* at § 2510(5)(a).

[67]*See id.* at § 2511(2)(d).

[68]*See id.* at § 2511(2)(a)(i). Specifically, the provider exception permits:

> An officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . .

Id.

[69]*See, e.g.*, Gantt, *supra* note 10, at 359.

[70]*See id.*

[71]*See id.*; *see also* Baum, *supra* note 1, at 1024.

The first court to apply the ECPA's provider exception in the context of e-mail monitoring in the workplace was the California Superior Court in *Flanagan v. Epson America*.[72] Although the case primarily involved alleged violations of the California Constitution and wiretapping law, the court addressed the applicability of the ECPA in a footnote.[73] The court stated that "there simply is no ECPA violation if 'the person or entity providing a wire or electronic communications service' intentionally examines everything on the system."[74] The clear implication of this statement is that the ECPA's provider exception would exempt an employer-provider from liability under the Act.[75]

The argument that employers can be deemed "providers" under the ECPA also finds support in *United States v. Mullins*.[76] In *Mullins*, an employee of American Airlines discovered a discrepancy on the computer reservations system, which later implicated a travel agent who had been making fictitious reservations.[77] The travel agent invoked the ECPA, arguing that American Airlines unlawfully intercepted the computer reservations.[78] The Ninth Circuit rejected the travel agent's claim, reasoning that as the provider of the system American Airlines was exempt from liability under the ECPA.[79] The Court concluded that under the provider exception, American Airlines was entitled to protect its rights and property.[80]

Finally, the most recent case lending support to the argument that employer-providers are immune from liability under the ECPA is *Bohach v. City of Reno*.[81] In *Bohach*, officers of the Reno Police Department pursued a cause of

---

[72]No. BC007036 (Cal. Super. Ct. 1991), *discussed in* Gantt, *supra* note 10, at 360.

[73]*See id.*

[74]*Id.* at n.100 (quoting Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 39 (1988)).

[75]*See* Gantt, *supra* note 10, at 360 (discussing Flanagan v. Epson America, No. BC007036 (Cal. Super. Ct. 1991)).

[76]992 F. 2d 1472 (9th Cir. 1992), *cert. denied*, 510 U.S. 994 (1993).

[77]*See id.* at 1475.

[78]*See id.* at 1478.

[79]*See id.*

[80]*See id.*

[81]932 F. Supp. 1232 (D. Nev. 1996). To date, *Bohach* is the most recent of all cases involving e-mail privacy in the workplace. *See* Baum, *supra* note 1, at 1030.

action alleging that the department's search of their messages sent over the department's computerized paging system violated the Fourth Amendment and federal wiretapping statutes.[82] The court likened the computerized paging system to e-mail and analyzed the officer's wiretapping claims under the ECPA.[83] After establishing that the Reno Police Department was the "provider" of the messaging service within the meaning of the provider exception, the court concluded that the provider exception "allows service providers to do as they wish when it comes to accessing communications in electronic storage."[84] Thus, the court held that neither the Reno Police Department nor its employees could be liable under the ECPA.[85]

The foregoing cases indicate that in the future, courts are likely to arrive at similarly broad interpretations of the provider exception to the ECPA. Intended or not, the provider exception to the ECPA has effectively eliminated e-mail privacy protection for employees who utilize company-owned e-mail systems. Indeed, an examination of the legislative history of the ECPA reveals that Congress' primary focus was on corporate privacy, not employee privacy.[86] Furthermore, the Senate report on the ECPA acknowledged the existence of company-owned e-mail systems, but "did not mention whether the Act would affect such systems."[87] As noted above, however, it remains an open question whether the provider exception would exempt an employer from liability who provides its employees e-mail service through a common carrier.[88]

---

[82]It appears that the police officers commenced this action in response to an internal affairs investigation involving the contents of the messages retrieved from the department's computer network. *See Bohach*, 932 F. Supp. at 1233. The officers sought to cease the investigation and to bar the disclosure of the contents of those messages. *See id.*

[83]*See id.* at 1234. The paging system used by the department "is like most pager systems, which store messages in a central computer until they are retrieved by, or sent to, the intended recipient." *Id.* The court explains that a message transmitted from the user's keyboard to the computer "is essentially electronic mail. . . ." *Id.*

[84]*Id.* at 1236.

[85]*See id.*

[86]*See* Gantt, *supra* note 10, at 362.

[87]*Id.*; *see also* Morris, *supra* note 17, at 340.

[88]*See* Gantt, *supra* note 10, at 359.

2. THE ORDINARY COURSE OF BUSINESS EXCEPTION

Another exception to the ECPA that may apply to e-mail communications in the private sector workplace is known as the ordinary course of business exception, or business extension exception.[89] This exception is essentially an exclusion from the definition of "electronic, mechanical or other device."[90] A prerequisite to a successful claim under the ECPA is that the alleged violator intercepted the electronic communication with an electronic device.[91] The ordinary course of business exception has yet to be applied to e-mail communications in the workplace.[92] Moreover, the legislative history of the ECPA is silent regarding how this exception may apply to e-mail communications.[93] Therefore, the only guidance available for this exception is an examination of its application in analogous contexts, such as to telephone communications.[94]

Courts applying this exception to telephone communications have followed two different approaches: a context approach or a content approach.[95] The content approach focuses on the nature of the communication and generally allows employers to monitor "business-related" communications, but disallows monitoring of "personal" communications.[96] On the other hand, the context

---

[89]*See* 18 U.S.C. § 2510(5)(a). The provision reads in pertinent part:

> 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.

[90]*Id.*

[91]*See id.* at § 2510(4). This section indicates that an interception can only occur through the use of an electronic or other mechanical device. *See id.*

[92]*See* Gantt, *supra* note 10, at 364-65; *see also* Dichter and Burkhardt, *supra* note 4.

[93]*See* Gantt, *supra* note 10, at 364.

[94]*See id.*

[95]*See id.* at 365.

[96]*Id.*; *see, e.g.*, Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (holding

approach focuses on the employer's reason for monitoring to determine whether a legitimate business reason justified the monitoring.[97]

The leading case to follow a context approach is *United States v. Harpel*.[98] In *Harpel*, the defendant appealed his conviction for "disclosing an unlawfully intercepted wire or oral communication" in violation of pre-ECPA Title III.[99] The defendant had allegedly recorded a telephone conversation between a police officer and agents of the Bureau of Narcotics and Dangerous Drugs.[100] Addressing the defendant's argument that the "ordinary course of business" exception exempted him from liability under Title III, the Tenth Circuit held that "a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business."[101] The court concluded that its holding "comports with the basic purpose of the statute, the protection of privacy . . . ."[102]

Similarly, the Eighth Circuit followed a context approach in *Deal v. Spears*.[103] In *Deal*, a private employee pursued a civil action against her employer for intercepting and disclosing the contents of personal telephone conversations.[104] The telephone calls were recorded by a device purchased by the employer that could be attached to an extension telephone in the employer's home.[105] The employer's stated purpose for monitoring the telephone calls was

---

that an employer cannot escape liability under the ordinary course of business exception for monitoring an employee's personal telephone call). *See* notes 127-38 and accompanying text for further discussion.

[97]*See* Gantt, *supra* note 10, at 365. *See, e.g.*, Sanders v. Robert Bosch Corp. 38 F.3d 736 (4th Cir. 1994) (holding that scant evidence of having received bomb threats would not justify an employer's covert and surreptitious monitoring of employee telephone calls). *See* notes 114-26 and accompanying text for further discussion.

[98]493 F.2d 346 (10th Cir. 1974).

[99]*Id.* at 348.

[100]*See id.*

[101]*Id.* at 351.

[102]*Id.*

[103]980 F.2d 1153 (8th Cir. 1992).

[104]*See id.* at 1155. The conversations revealed that the employee was having an extramarital affair. *See id.*

[105]*See id.* The machine automatically recorded all incoming or outgoing calls, "with no

suspicion that one of its employees was responsible for a recent burglary.[106] The only evidence of employee wrongdoing uncovered by the twenty-two hours of recordings was an employee's admission of having sold a keg of beer at cost.[107]

The employer argued that it was immune from liability under Title III because its actions fell under the ordinary course of business exception.[108] The court rejected the employer's rationale that the extension telephone used to intercept the calls was "furnished to the subscriber or user by a provider of wire or electronic communication service" within the meaning of the exception.[109] Instead, the court noted that the calls were intercepted by the recording device purchased by the employer, which was not provided by the telephone company.[110] Furthermore, the court determined that the monitoring was not conducted in the ordinary course of business.[111] The court observed that even though the employer had a legitimate business interest in monitoring to prevent theft, the employer had no business interest in listening to the entire twenty-two hours of recorded conversations which were largely personal in nature.[112] Thus, the court concluded that the "extent of the intrusion" or "scope of the interception" exceeded the boundaries of the ordinary course of business exception.[113]

---

indication to the parties using the phone that their conversation was being recorded." *Id.*

[106]*See id.*

[107]*See id.* at 1156. The record did not indicate whether any information was learned about the burglary. *See id.* Apparently, selling the keg of beer at cost was a violation of store policy. *See id.* It was on this basis that the employer confronted the employee with the tape recordings and then terminated her employment. *See id.*

[108]*See id.* at 1157. The employer also argued that it was immune from liability because the employee consented to the interception. *See id.* at 1156. See Part II, Section B, subsection 3 of this Comment for an analysis of the consent exception to the ECPA.

[109]*Id.* at 1157.

[110]*See id.* ("We hold that the recording device, and not the extension phone, intercepted the calls.").

[111]*See id.* at 1158.

[112]*See id.* The court noted that the employer "might legitimately have monitored Deal's calls to the extent necessary to determine that the calls were personal and made or received in violation of store policy." *Id.*

[113]*Id.*

The most recent case applying the ordinary course of business exception to the ECPA also followed the context approach.[114] In *Sanders v. Robert Bosch Corp.*, the employer had installed a telephone recording device known as a 'voice logger,' which continuously recorded all telephone conversations on certain telephone lines.[115] The employer cited bomb threats as the reason for installing the voice logger device.[116] Upon learning that her personal calls had been monitored, the plaintiff employee brought suit against the employer under Title III for the surreptitious recording of her telephone conversations.[117] The employer claimed immunity from liability under the ordinary course of business exception.[118]

The United States Court of Appeals for the Fourth Circuit noted that in order for the exception to apply, it must first be established that the voice logger constitutes a "telephone or telegraph instrument" or other electronic device furnished by a provider of such service in the ordinary course of its business.[119] Second, the employer's use of the device must be made in the ordinary course of business.[120] The court found that neither prong was satisfied under the facts of the case.[121] In finding that the first prong was not met, the court explained that the voice logger was added by the employer, and not the telephone service provider.[122] The court reasoned that the employer failed to satisfy the second prong because the surreptitious recording of phone lines on the basis of having received bomb threats could not fall within the ordinary course of the employer's business.[123] The scant evidence of bomb threats in the first place led the court to "question whether the record evidences a business justification for

---

[114]*See* Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994).

[115]*See id.* at 737.

[116]*See id.* at 738.

[117]*See id.* at 737. It should also be noted that the employer did not inform any nonsupervisory personnel of the telephone recordings. *See id.* at 738.

[118]*See id.* at 740.

[119]*Id.* at 740 (citing Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992)).

[120]*See id.*

[121]*See id.* at 741.

[122]*See id.* at 740.

[123]*See id.* at 741.

the drastic measure of 24-hour a day, 7-day a week recording of telephone calls."[124]

Moreover, the Fourth Circuit's consideration of the covert nature of the monitoring is also noteworthy. In addressing the fact that the employer never informed its non-supervisory employees of the monitoring, the court stated that "[i]n light of the Act's clear purpose of protecting individuals' privacy interests, the determination of whether the 'use' made of a surveillance device falls within the ordinary course of business so as to satisfy section 2510(5)(a)(i) necessarily entails examination of whether such 'use' was covert or open."[125] The court proceeded to suggest that the employer must invoke a legitimate business reason for covert monitoring.[126]

The leading case to apply the ordinary course of business exception following a content approach is *Watkins v. L.M. Berry & Co.*[127] In *Watkins*, an employee brought suit against her employer for monitoring a personal telephone call she received while on her lunch break.[128] The employer maintained a telephone solicitation business and had an established policy of monitoring solicitation calls made by its employees.[129] All employees were informed of this policy as it was part of the training program for the employer to record the solicitation calls and offer feedback to the employees.[130] Furthermore, employees were permitted to make personal calls and were informed that personal calls would not be subject to monitoring.[131] The employee brought suit under Title

---

[124]*Id.*

[125]*Id.*

[126]*See id.* at 741-42. The court appeared to be questioning the legitimacy of the covert nature of the monitoring rather than of the monitoring itself.

[127]704 F.2d 577 (11th Cir. 1983).

[128]*See id.* at 579. The telephone call was received from a friend of the employee. *See id.* The subject of the conversation was an employment interview that the employee "had had with another company." *Id.* The next day she was confronted by a supervisor who indicated that she knew about the interview with the other company. *See id.*

[129]*See id.* The monitoring was "accomplished with a standard extension telephone, located in the supervisor's office, which shares lines with the telephones in the employee's offices." *Id.*

[130]*See id.*

[131]*See id.* The employees were informed that personal calls would only be monitored to the extent necessary to determine whether the call was personal or business-related. *See id.*

III and the employer argued that it was exempt from liability under the ordinary course of business exception.[132]

The court conceded that the employer's monitoring of solicitation calls was within its ordinary course of business.[133] Thus, the issue was whether the interception of the plaintiff's personal call was within the employer's ordinary course of business.[134] The court concluded that the intercepted telephone call in this case was not likely to be construed as a business or solicitation call.[135] The court unequivocally held that the ordinary course of business exception would not immunize an employer for intercepting a personal call, except for the purpose of determining whether the call is personal or to prevent unauthorized use of the telephone.[136] "In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents."[137] This obligates the employer to cease monitoring after it learns of the personal nature of the telephone call.[138]

Similarly, in *Epps v. St. Mary's Hospital of Athens, Inc.*,[139] the court followed the content approach in applying the ordinary course of business exception. In *Epps*, the employee brought a Title III action against his employer and one of its employees, individually, for recording a telephone conversation in which the plaintiff made disparaging comments about two supervisors.[140] The conversation took place on a telephone in the Emergency Medical Services ("EMS") office.[141] In response to the defendants' argument that the ordinary

---

[132]*See id.* at 579-80. The employer also argued that plaintiff's acceptance of the monitoring policy constituted her consent to being monitored. *See id.* at 580. See Part II, Section B, subsection 3 of this Comment for an analysis of the consent exception to the ECPA.

[133]*See id.* at 582 ("It is not enough for Berry Co. to claim that its general policy is justifiable as part of the ordinary course of business. We have no doubt that it is.").

[134]*See id.*

[135]*See id.*

[136]*See id.* at 583.

[137]*Id.*

[138]*See id.* at 584. The court indicated that the appropriate time to cease monitoring is to be determined by the trier of fact. *See id.*

[139]802 F.2d 412 (11th Cir. 1986).

[140]*See id.* at 413.

[141]*See id.*

course of business exception immunizes it from liability for monitoring phone calls, the plaintiff argued that the hospital's monitoring policy encompassed only incoming and outgoing calls from the dispatch console, not from the hospital's EMS office.[142] The defendants asserted that the recording was undertaken in the ordinary course of business because the content of the conversation involved employee relations.[143]

In holding that this telephone call was not of a personal nature, the court noted that "[the conversation] occurred during office hours, between co-employees, over a specialized extension which connected the principal office to a substation, and concerned scurrilous remarks about supervisory employees in their capacities as supervisors."[144] The court reasoned that an employer has a legal interest in "the potential contamination of a working environment."[145] Thus, the employer was immune from liability under Title III.[146]

Having analyzed the context and content approaches to the application of the ordinary course of business exception in the telephone monitoring context, some predictions may be made regarding its application to e-mail communications. Courts following the context approach would likely deem the interception of employees' personal e-mail messages to fall outside the ordinary course of business exception to the ECPA.[147] The interception of personal e-mail

---

[142]*See id.* at 416.

[143]*See id.*

[144]*Id.* at 417.

[145]*Id.* The court cited *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 583-84 (11th Cir. 1983) for the proposition that a personal call is one in which an employer has no legal interest in the contents of the conversation. *See Epps*, 802 F.2d at 416-17. The court explained that:

> Berry Co. might have been curious about Watkins' plans, but it had no legal interest in them. Watkins was at liberty to resign at will and so at liberty to interview with other companies. Her interview was thus a personal matter, neither in pursuit nor to the legal detriment of Berry Co.'s business . . . .

Id. at 416; *see also* notes 131-41 and accompanying text.

[146]*See id.* at 417.

[147]*See* Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994); Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992); United States v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974).

messages would only be permitted to the extent necessary to determine the personal nature of the messages.[148] In addition, the *Sanders* case suggests that the surreptitious monitoring of employee e-mail communications, without informing employees of potential monitoring, will rarely be justified under the ordinary course of business exception.[149]

Courts following the content approach may permit the interception of employee e-mail communications if the employer can establish a legal interest in the subject matter of the communications.[150] The *Epps* case suggests that any e-mail communications containing disparaging remarks about supervisory personnel may implicate a legitimate, legal interest of the employer, which would immunize the employer from liability for monitoring under the ordinary course of business exception.[151] Conversely, it appears that the content approach would not permit employer monitoring of employee e-mail communications that are purely personal in nature and do not implicate a legal interest of the employer.[152]

3. THE CONSENT EXCEPTION

The consent exception to the ECPA generally applies in the event that one party to the communication has given prior consent to the interception or accession of the communication.[153] Thus, so long as the communication is inter-

---

[148]*See supra* note 112 and accompanying text.

[149]*See supra* notes 117-130 and accompanying text.

[150]*See* Epps v. St. Mary's Hospital of Athens, Inc., 802 F.2d 412, 417 (11th Cir. 1986); *Watkins*, 704 F.2d at 583.

[151]*See supra* notes 139-46 and accompanying text.

[152]*See supra* notes 127-46 and accompanying text.

[153]Specifically, this exception provides that:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution of laws of the United States or of any State.

18 U.S.C. § 2511(2)(d) (1994).

cepted by a person who is either a party to the communication or has given prior consent to such interception, the prohibitions contained in the ECPA will not apply.

This exception was interpreted by the Eleventh Circuit in *Watkins*.[154] In *Watkins*, the court determined that the scope of the employees' consent extended only to the employer's policy of monitoring business calls and personal calls only to the extent necessary to determine the personal nature of the call.[155] The Eleventh Circuit refused to accept the employer's argument that the employee's knowledge of a monitoring policy was sufficient to imply consent.[156] The court concluded that consent was "not necessarily an all or nothing proposition," and that it could be limited.[157]

The permissible scope of the consent exception was also considered in *Deal v. Spears*.[158] In *Deal*, the employer had informed the employee on one occasion that it might resort to monitoring her phone calls as a result of the employee's extensive personal use of the telephone.[159] The court cited *Watkins* for the proposition that an employee's knowledge of the employer's capability of monitoring is not sufficient to imply consent.[160] The court reasoned that the employer never informed the employee that it would be monitoring her calls, but only that it might monitor her calls.[161] Thus, the employer was unable to escape liability under the consent exception to Title III.[162]

---

[154]*See* 704 F.2d 577 (11th Cir. 1983). *See also* notes 127-38 and accompanying text. Recall in *Watkins*, the employer informed its employees that all telephone solicitation or business calls were subject to monitoring. *See Watkins*, 704 F.2d at 579. On the other hand, personal calls were permitted and the employees were informed that personal calls would only be monitored to the extent necessary to determine the personal nature of the call. *See id.*

[155]*See id.* at 581.

[156]*See id.*

[157]*Id.* at 582.

[158]980 F.2d 1153 (8th Cir. 1992); *see also* notes 103-113 and accompanying text.

[159]*See Deal*, 980 F.2d at 1155-56.

[160]*See id.* at 1157; *see also* notes 154-57 and accompanying text.

[161]*See Deal*, 980 F.2d at 1157.

[162]*See id.*

These two cases suggest that consent may be actual or implied.[163] More importantly, *Watkins* and *Deal* suggest that an employer may successfully evade the prohibitions of the ECPA by publishing a monitoring policy.[164] As applied to e-mail communications, employees' acceptance of a monitoring policy reserving to the employer the right to monitor employee e-mail would constitute consent, thus immunizing the employer from liability for monitoring under the ECPA. The foregoing cases do, however, recognize that consent may be limited under the circumstances. For example, an employer who informs its employees that all business-related e-mail is subject to monitoring will not be able to successfully argue that employees' mere knowledge of a monitoring policy constituted their consent to the monitoring of personal e-mail.

The uncertainty surrounding the application of the ECPA to e-mail monitoring in the private sector workplace prompted several Congressional leaders to introduce the Privacy for Consumers and Workers Act ("PCWA")[165] in 1993.[166] Essentially, this Act would require employers to inform its employees of workplace monitoring and place limits on the extent to which an employer may monitor.[167] The bill also provides that an adverse employment action may not be taken against an employee based on information the employer obtained in violation of the provisions of the PCWA.[168]

The proposed PCWA has been criticized for the vagueness of its terms and the administrative burden it would impose upon employers.[169] A further criticism of the PCWA is its reliance upon length of service as the basis for privacy protection.[170] If the purpose of the Bill is to protect employee privacy, then the

---

[163]*See* Gantt, *supra* note 10, at 356.

[164]*See id.* at 357-58.

[165]*See* H.R. 1900, 103rd Cong., 1st Sess. (1993).

[166]*See* Lehman, *supra* note 13, at 104; Dichter and Burkhardt, *supra* note 4.

[167]*See* H.R. 1900, 103rd Cong. § 4 (1993).

[168]*See* H.R. 1900 § 8.

[169]*See* Lehman, *supra* note 13, at 104.

[170]The proposed legislation would provide:

> (1) New Employees.—An employer may engage in random and periodic monitoring of an employee of such employer if the cumulative total period of such employee's employment is not more than 60 days.

more appropriate focus is on restricting employers, not on distinctions among employees' length of service. Ostensibly, the length of service distinctions serve as a compromise to employers, but it exemplifies the likely resistance that employee privacy legislation will face at the federal level. To date, Congress has not enacted the proposed PCWA, and no further action has been taken.[171]

C. COMMON LAW TORT CAUSES OF ACTION

Due to the lack of clear constitutional or statutory protection, the primary source for employee privacy protection in the private sector workplace is likely state tort law.[172] The Restatement (Second) of Torts[173] recognizes four distinct torts protecting the right of privacy: "unreasonable intrusion upon the seclusion of another . . . appropriation of the other's name or likeness . . . unreasonable publicity given to the other's private life . . . or publicity that unreasonably places the other in a false light before the public."[174]

The tort most likely implicated by e-mail monitoring in the workplace is the "intrusion upon seclusion" tort.[175] This tort provides that "one who intention-

---

> (2) Other Employees.—An employer may not engage in random and periodic monitoring of an employee with a cumulative employment period with such employer of at least 5 years.
>
> (3) Work Groups.—An employer may engage in electronic monitoring of an employee of such employer who has a cumulative employment period with such employer of less than 5 years and who is in a work group of employees on a periodic or random basis for not more than 2 hours in any week . . . [N]otice to each employee within such work group for such monitoring shall be provided at least 24 hours but not more than 72 hours before engaging in such monitoring. . . .

H.R. 1900, 103rd Cong. § 5 (1993).

[171] *See* Dichter and Burkhardt, *supra* note 4.

[172] *See also* Gantt, *supra* note 10, at 373; Dichter and Burkhardt, *supra* note 4. These commentators suggest that state tort law provides the greatest protection for e-mail privacy in the workplace. *See id.*

[173] RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[174] *Id.*

[175] *See id.*; Lehman, *supra* note 13, at 104. In theory, this tort would apply when an

ally 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."[176] In holding that the invasion may be "physical or otherwise", this tort may be extended to protect against e-mail monitoring.[177] This tort also imposes a standard of objective reasonableness. Thus, "[i]n deciding whether the intrusion is into a private matter, courts require not only that the employee have a subjective expectation of privacy but also that the expectation be objectively reasonable."[178]

The common law tort of invasion of privacy has been applied in two cases involving e-mail monitoring in the workplace. The first such case was *Bourke v. Nissan Motor Corp.*,[179] an unreported California decision. In *Bourke*, the plaintiffs brought an action against their employer for intercepting and reviewing several personal e-mail messages.[180] In rejecting the plaintiffs' claim for tortious invasion of privacy, the court held that the employees did not have a reasonable expectation of privacy in their e-mail because the employees had signed a waiver form stating that e-mail use was limited to "company business."[181] Also, the court noted that the employees were aware that other coworkers had read their e-mail messages in the past, even though they were not the intended recipients of those messages.[182] The court further rejected the plaintiffs' argument that a subjective expectation of privacy existed by virtue of having personal passwords to access the e-mail system and being told to safe-

---

employer intercepts, but does not disclose, an employee's e-mail messages. *See* Gantt, *supra* note 10, at n.190. In the event that the contents of an employee's e-mail messages are disclosed, an employee may have a cause of action under the "unreasonable publicity given to the other's private life" or, depending on the nature of the contents, "publicity that unreasonably places the other in a false light before the public." *See id.*

[176]RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[177]*See also* Gantt, *supra* note 10, at 374.

[178]*Id.* at 375.

[179]No. YC003979 (Cal. Super. Ct. App. 1991), *discussed in* Paul E. Hash and Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 907 (1996).

[180]*See id.*

[181]*See id.*; Dichter and Burkhardt, *supra* note 4; Gantt, *supra* note 10, at 378.

[182]*See Bourke*, No. YC003979, *discussed in* Hash and Ibrahim, *supra* note 179, at 907.

guard those passwords.[183]

The most recent case to address the common law tort of invasion of privacy was *Smyth v. Pillsbury Co.*[184] In *Smyth*, the employee brought suit against his employer for wrongful discharge.[185] The employee was discharged after company executives reviewed the contents of his e-mail messages which contained offensive references toward the company's sales management.[186] The employee had sent these messages to a supervisor in the company in reliance upon the company's policy that all e-mail communications would remain private and confidential.[187] The plaintiff-employee argued that his termination was against public policy as a violation of his common law right to privacy.[188]

The court analyzed the plaintiff's claim under the Restatement (Second) definition of intrusion upon seclusion.[189] In doing so, the court found that the plaintiff could not have "a reasonable expectation of privacy in e-mail communications voluntarily made . . . to his supervisor over the company e-mail system."[190] Secondly, the court found that even if the employee was determined to have a reasonable expectation of privacy in the contents of his e-mail messages, the court would not "consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy."[191] The court concluded by adding that any privacy interest of the employee was outweighed by the employer's "interest in preventing inappropriate and unprofessional comments . . . over its e-mail system."[192]

As the only cases applying the common law invasion of privacy tort to e-mail monitoring, *Bourke* and *Smyth* provoke a grim outlook for e-mail privacy

---

[183]*See id.*

[184]914 F. Supp. 97 (E.D. Pa. 1996).

[185]*See id.* at 98.

[186]*See id.* at 99 n.1.

[187]*See id.* at 98.

[188]*See id.* at 100.

[189]*See id.* at 100-01 (relying on RESTATEMENT (SECOND) OF TORTS § 652B (1977)).

[190]*Id.* at 101.

[191]*Id.*

[192]*Id.*

in the workplace. The above-cited cases suggest that courts will provide a very narrow reading of employees' reasonable expectation of privacy. The *Bourke* case holds that maintaining a personal password to access the e-mail system does not give rise to an objectively reasonable expectation of privacy.[193] The *Smyth* case indicates that even an employer's stated policy that employee e-mail is private and confidential will not necessarily give rise to an objectively reasonable expectation of privacy.[194] Thus, to this point, the state of the common law with respect to e-mail monitoring in the workplace clearly favors employers.

III. CONCLUSION

The constitutional provisions, statutory enactments and tort causes of action examined in this Comment highlight the inadequacy of existing law in protecting e-mail privacy in the workplace. Although the federal constitution and various state constitutions offer some level of privacy protection to public employees,[195] private employees must rely exclusively on federal and state statutory law or common law tort causes of action.[196] The ineptitude of the ECPA, coupled with the unwillingness of courts to recognize a zone of privacy in employee e-mail communications, is cause for concern.

Existing law and precedent offer extremely narrow circumstances in which an employee may find vindication for the invasion of their e-mail privacy. In spite of the ECPA's general ineffectiveness as applied to e-mail communications in the workplace, there remains a possibility of finding employer liability for e-mail monitoring under the Act.[197] This possibility would exist if the employer provided e-mail service to its employees through a common carrier, and did not maintain an e-mail policy governing employee usage of the e-mail service. The provision of service through a common carrier may successfully counter the argument for employer immunity under the provider exception to the ECPA.[198] Furthermore, the absence of a written e-mail policy may render

---

[193]*See supra* notes 179-183 and accompanying text.

[194]*See supra* notes 184-192 and accompanying text.

[195]*See supra* notes 23-38 and accompanying text.

[196]See Part II, Section A of this Comment for an analysis of private employees' constitutional protections.

[197]*See supra* notes 71 and 88 and accompanying text.

[198]*See id.* See Part II, Section B, subsection 1 of this Comment for an analysis of the provider exception to the ECPA.

the consent exception to the ECPA inapplicable.[199]

The remaining obstacle to finding employer liability would be the ordinary course of business exception to the ECPA. An employer could escape liability under this exception by demonstrating either a legal interest in the subject matter of the communication or some other legitimate justification for monitoring, such as to insure compliance with an established e-mail policy.[200] However, this exception could be overcome by evidence that the employer monitored e-mail communications that were purely personal in nature and did not implicate a legal interest of the employer.[201] The ordinary course of business exception would also fail to immunize an employer who conducts monitoring in contravention of a written e-mail policy.[202]

It should be noted that a written e-mail policy may not only immunize an employer from liability under the ECPA, but may also immunize an employer from tort liability for invasion of privacy. In fact, the only two tort cases involving e-mail privacy in the workplace expressly and impliedly stand for the proposition that a written e-mail policy will be sufficient to render unreasonable any expectation of privacy.[203] This precedent effectively bestows upon employers the power to write their own laws on this issue, via the written e-mail policy.[204]

---

[199]See Part II, Section B, subsection 3 of this Comment for an analysis of the consent exception to the ECPA.

[200]See Part II, Section B, subsection 2 of this Comment for an analysis of the ordinary course of business exception to the ECPA.

[201]*See id.*

[202]*See id.*

[203]*See* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); *Bourke*, No. YC003979 (Cal. Super. Ct. 1991), *discussed in* Hash and Ibrahim, *supra* note 179, at 907;. See Part II, Section C of this Comment for an analysis the common law tort of invasion of privacy.

[204]The following is a sample of the language contained in an e-mail policy:

ELECTRONIC MAIL POLICY

* E-mail is the property of the company and should be used solely for work-related purposes.

* Employees are prohibited from sending messages that are harassing, intimi-

Indeed, "recent inventions and business methods" are calling attention to the steps which must be taken for the protection of employee privacy. Unfortunately, the law with regard to e-mail privacy in the workplace is reliant upon employers to take those steps. It is unrealistic to expect employers to voluntarily recognize and respect the privacy of employee e-mail communications. Moreover, it is unlikely that courts will be willing to overrule such recent

---

dating, offensive or discriminatory. Such conduct by an employee may result in immediate dismissal or other disciplinary measures.

* Each employee will be given a password to access e-mail. Your password is personal and should not be shared with anyone else. Employees are prohibited from accessing someone else's E-Mail. However, the company retains a copy of all passwords and has a right to access E-Mail at any time for any reason without notice to the employee. The Employee has no expectation of privacy or confidentiality in the E-Mail system.

* The employee must sign and return an Acknowledgment & Consent form indicating receipt and acceptance of our company's policy.

Acknowledgment

I understand that the company's electronic mail and voice mail systems (herein together referred to as "the company's systems) are company property and are to be used for company business. I understand that [excessive] use of the company's systems for the conduct of personal business is strictly prohibited.

I understand that the company reserves the right to access, review, and disclose information obtained through the company's systems at any time, with or without advance notice to me and with or without my consent. I also understand that I am required to notify my supervisor and the company's Security Department if I become aware of any misuse of the company's systems.

I confirm that I have read this employee acknowledgment and have had an opportunity to ask questions about it. I also agree to abide by the terms of the company's policy in this regard, a copy of which has been provided to me.

AGREED TO THIS ____ DAY OF _____, 199__.

Robert B. Fitzpatrick, *Technology Advances in the Information Age: Effects on Workplace Privacy Issues*, SC08 ALI-ABA 599, 625 (July 17, 1997) (emphasis added).

precedents as those involving e-mail privacy in the workplace. Thus, it is incumbent upon Congress or the individual state legislatures to reverse the current trend toward unrestricted employer monitoring. In so doing, our elected officials should be guided by the notion that "[w]e are a nation of employees."[205] This proclamation serves as a reminder that the policies of the workplace should at least resemble the policies of our nation.

[205]Pierce v. Ortho Pharmaceutical Corp., 84 N.J. 58, 66, 417 A.2d 505, 509 (1980) (recognizing the general public policy of protecting employees from abusive employer practices); *accord* Woolley v. Hoffman-La Roche, Inc., 99 N.J. 284, 292, 491 A.2d 1257, 1261 (1985); *see* Nicosia v. Wakefern Food Corp., 136 N.J. 401, 419, 643 A.2d 554, 563 (1994).