WORKPLACE E-MAIL: IT'S NOT AS PRIVATE AS YOU MIGHT THINK

ABSTRACT

The modern workplace has dramatically changed in the last two decades with the dawn of the technological revolution. One notable change has been the widespread use of e-mail in the workplace, as a means of both business and personal communication. Courts across the country have recently been called upon to decide just what, if any, privacy an employee can expect in her e-mail, particularly when weighed against the employer's right to monitor the workplace. Most office employees falsely assume that the e-mail messages they send and receive are private and confidential. Actually, e-mail sent or received via the employer's e-mail system is increasingly subject to company control and monitoring. This comment examines what existing law protects an employee's right to privacy in her e-mail. A brief look at possible Constitutional protections is followed by an examination of the most commonly-invoked statute in this area, the Electronic Communications Privacy Act of 1986. The emerging caselaw on this subject is also examined, with the conclusion that employees generally have no expectation of privacy in their workplace e-mail. Finally, this comment offers suggestions on how employees can protect their privacy and businesses can guard against lawsuits and retain control of their workplace.

I. INTRODUCTION

The modern workplace has dramatically changed in the last two decades with the dawn of the technological revolution. One notable change has been the widespread use of electronic mail (e-mail)\(^1\) as a means of both intra-company communication and as a source of communication with the outside client base.\(^2\) E-mail has made disseminating information among

---

\(^1\)In Senate discussions surrounding the enactment of the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22, 2701-10, 3117, 3121-26 (1994), e-mail was described as technology that enables two parties to communicate through the transmission of digital messages over public or private telephone lines. The e-mail message is then held in a computer "mail box" until it is retrieved by the recipient. See S. REP. NO. 99-541, 99th Cong., 2d Sess. (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3562. See Kevin P. Kopp, Comment, Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy, 8 SETON HALL CONST. L. J. 861, 862-63 n.3 (1998).

\(^2\)While the exact numbers are constantly changing, a recent poll found that over forty million employees use e-mail and the number is estimated to grow 20% every year. See Kopp, supra note 1, at 862 (citing Mark S. Dichter & Michael S. Burkhardt, Electronic Interaction in the
employees much easier; no longer must hundreds of copies of a written memorandum be distributed, nor departmental meetings be held, to notify employees of a minor change in policy. With a few clicks of a button, a message is sent from the office of the manager to the desktop computer terminals of all her employees. The ease of this form of communication is enticing. For employees, it provides a means of passing along not only work-related ideas but the latest company gossip as well, all without ever having to leave their desks.

It is against this backdrop that courts across the country have recently had to decide what privacy, if any, an employee has in her e-mail, particularly when weighed against the employer's right to monitor the workplace. Most office employees assume an e-mail message to be private and confidential, no different than if it were a written letter sent in a sealed envelope. Like traditional mail, e-mail is sent to a designated recipient who traditionally goes through a sign-on process, including entry of a personal password to get to her "mailbox" where the e-mail message is stored until she opens it so it can be read.

There are, however, significant differences between traditional mail and e-mail systems. For example, "e-mail messages are, by definition, stored

---

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) (citing a recent survey conducted by the Gallup Organization). It has also been estimated that 90% of large companies, 64% of mid-size companies, and 42% of small companies have e-mail systems in place. Id. Predictions are that by the year 2000, approximately 60 million electronic mail users will be transmitting 60 billion messages per year. See Alexander I. Rodriguez, Comment, All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace, 47 EMORY L.J. 1439, 1439 n.3 (1998) (citing Scott Dean, E-Mail Forces Companies to Grapple With Privacy Issues, CORP. LEGAL TIMES, Sept. 1993, at 11).

See Kopp, supra note 1, at 862 (citing Steven Miller, E-Mail's Popularity Poses Workplace Privacy Problems, BUS. FIRST OF COLUMBUS, Oct. 3, 1997). See also C. Forbes Sargent, III, Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues, 41 BOSTON B.J. 6, 6-7 (May/June 1997) (commenting on increased use and popularity of workplace e-mail).

See Sargent, supra note 3, at 6 (noting that e-mail "technology has greatly facilitated communication in the office, [and] in many instances replaced the hand-written note or discussion by the water cooler").


See Sargent, supra note 3, at 6 ("[T]he common assumption is that e-mail is as private and confidential as communication via the U.S. Postal Service.").
in a routing computer" and are accessible by a system administrator.\textsuperscript{8} Employees are routinely unaware of these differences.\textsuperscript{9} Furthermore, e-mail sent or received via the company's e-mail system, or a system the company pays a third party to provide to its employees, is increasingly subject to company control and monitoring.\textsuperscript{10} A recent study found that thirty-two percent of employers who provide e-mail randomly monitor their employee's transmissions,\textsuperscript{11} which in light of employee assumptions is particularly surprising.

This comment will examine what existing law protects an employee's right to privacy in her e-mail. Part II will look at possible constitutional protections and will be followed by an examination of relevant federal and state statutes. The most commonly-invoked statute in this area is the Electronic Communications Privacy Act of 1986 (ECPA).\textsuperscript{12} Finally, Part III of this comment will offer suggestions on how employees can protect their

\textsuperscript{8}Bohach, 932 F. Supp. at 1234 (citation omitted); see also Kopp, supra note 1, at 862-63 n.10.

\textsuperscript{9}See Bohach, 932 F. Supp. at 1234 n.2. See also Larry O. Natt Gantl, II, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 HARV. J.L. & TECH. 345, 349 (1995) (noting that many employees remain unaware that the central computer routing the e-mail messages stores the transmission in unencrypted plain text files, available to the service provider whether that be a third-party common carrier or the employer itself). See also Sargent, supra note 3, at 6 (arguing that although instant storage of information has increased workplace productivity and saved many inadvertently deleted documents, it has also led to invasions of employee privacy). Most employees do not know that the e-mail system stores all messages automatically. Furthermore, most systems are accessible to the network administrator and other designated personnel, providing the opportunity to monitor all e-mail and documents stored on the system. Id.

\textsuperscript{10}There are many reasons why an employer may wish to monitor its employees private e-mail communications, particularly to limit employee abuses or misuses of the e-mail system. See Kopp, supra note 1, at 863 (citing Jarrad J. White, E-Mail@Workcom: Employer Monitoring of Employee E-Mail, 48 ALA. L. REV. 1079, 1079-80 (1997)). The abuses could range from simply sending personal messages during work hours to sending harassing messages or revealing company secrets to other companies. Id. at 863-64.

\textsuperscript{11}The Society for Human Resource Management conducted the study and derived the statistics from a poll of 538 business executives. See Kopp, supra note 1, at 862 (citing Liz Halloran, Big Brother is Reading This: Your Boss Can Browse Your E-Mail, HARTFORD COURANT, Apr. 15, 1996, at A1). Another study found that 25\% of employers who monitor their employee's e-mail do not inform their employees that they may be monitored. Id. at 863 n.11 (citing 5 TELECOM & NETWORK SEC. REV., No. 6 (June 1, 1997) (noting that the survey was administered to 900 American Management Association member companies)). There are software programs on the market that actually assist employers in monitoring large amounts of employee e-mail. Id. at 862-63 n.10 (citing Amitai Etzioni, Some Privacy, Please, For E-Mail, CHI. DAILY L. BULL., Nov. 24, 1997, at 6). The programs work by detecting keywords in the text of the e-mail that signal certain types of behavior or communication that the company wants to control or prohibit. After the program scans all employee e-mail, the communications containing the targeted words are retrieved for the employer to read in their entirety. See id.

privacy and employers can guard against lawsuits and retain control of their workplace.

II. BACKGROUND

A. Constitutional Protections

The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures by government officials. Although the Fourth Amendment does not explicitly mention a right to privacy, the Supreme Court has long interpreted it to include protection of such a right. The Fourth Amendment only restrains the conduct of governmental actors, in other words, it provides protection for governmental employees but is of little help to the vast majority of employees who work in the private sector. Even for governmental employees, the Fourth Amendment offers only limited protection from workplace searches.

This being the case, it may seem meaningless to discuss the Fourth Amendment in the context of employee privacy rights in their workplace e-mail. Constitutional jurisprudence, however, has influenced judges when considering invasion of privacy cases arising under state constitutions, statutes, and common law. For example, the test of reasonableness derived from the seminal case of Katz v. United States is employed in common law

---

13The text of the Fourth Amendment reads, 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." U.S. CONST. amend. IV.

14See Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (declaring unconstitutional a statute banning the use of contraceptives based on the right to privacy protected implicitly by the Bill of Rights, including the Fourth Amendment). See also Katz v. United States, 389 U.S. 347, 359 (1967) (holding that electronic surveillance of a phone booth, without a warrant, violated the Fourth Amendment, which protects against unreasonable searches and seizures).


16See O'Connor v. Ortega, 480 U.S. 709 (1987) (finding a government employee's expectation of privacy unreasonable when the government actor is the employee's supervisor). The Fourth Amendment is only violated if public employees have a reasonable expectation of privacy. This standard requires balancing the employer's need for control and supervision of the workplace against the privacy interests of its employees. Id. See also Steven B. Winters, Note, Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail, 1 S. CAL. INTERDISC. L.J. 85, 116 (1992) (arguing that federal courts have so narrowly construed the public employees' work-related privacy rights that the right of privacy has almost completely vanished).

17See Rodriguez, supra note 2, at 1445.

18See id. See also Gantt, supra note 9, at 380 (stating that the test in tort cases of invasion of privacy is the same as the balancing test under the Fourth Amendment).

invasion of privacy tort claims. Therefore, one can move quickly past the Fourth Amendment when analyzing employee privacy rights in their workplace e-mail.

Eight states' constitutions explicitly protect privacy and offer greater protection of the rights of public employees. As with the United States Constitution, however, the state law only protects public employees and the protections do not extend to the private sector. The one and only notable exception to this rule is the state of California, that has extended its state constitution's protection of privacy to private as well as public employees.

B. Statutory Protection

Since neither the United States Constitution nor any state constitution is adequate to protect most employees' privacy in their workplace e-mail, many have looked to the legislatures for protection. Attempting to answer the outcry of many aggrieved employees, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA prohibits the intentional or willful interception, accession, disclosure, or use of one's electronic communication. This statute is the only federal statute that specifically addresses e-mail interception and monitoring.

\[^{20}\text{See infra text accompanying notes 60-63. See also Julia Turner Baumhart, The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?, 8 LAB. LAW. 923, 938 (1992) (noting that private employers should consider Fourth Amendment cases when trying to protect against invasion of privacy claims).}\]

\[^{21}\text{See Kopp, supra note 1, at 867 n.36 (citing the constitutions of Alaska, California, Florida, Hawaii, Illinois, Louisiana, Montana, and Washington).}\]

\[^{22}\text{See Porten v. University of San Francisco, 134 Cal. Rptr. 839, 842 (Cal. Ct. App. 1976) (recognizing a state constitutional violation even when there is no state action).}\]

\[^{23}\text{See Kevin Baum, Comment, E-Mail in the Workplace and the Right of Privacy, 42 VILL. L. REV. 1011, 1018 (1997).}\]

\[^{24}\text{Pub. L. No 99-508, 100 Stat. 1848, as amended, 18 U.S.C. §§ 2510-22, 2701-10, 3117, 3121-26 (1994). The ECPA was enacted in response to a 1985 Office of Technology Assessment report that emphatically expressed the threat unregulated invasions into electronic communications had on personal privacy. See White, supra note 10, at 1080-81. See also Gantt, supra note 9, at 857 (discussing the legislative history of ECPA).}\]

\[^{25}\text{See 18 U.S.C. § 2511 (1994). See also Kopp, supra note 1, at 868-70 (stating that the ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and when the ECPA is read with Title III intentional or willful interception of wire, oral, or electronic communication is prohibited).}\]

\[^{26}\text{The ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate commerce." 18 U.S.C. § 2510(12) (1994). Although e-mail is not specifically mentioned here, the legislative history clearly shows Congress' intent to include it within the definition of "electronic communications." See Kopp, supra note 1, at 868 n.46 (citing Dichter & Burkhardt, supra note 2).}\]
Although the ECPA does not, by its terms or legislative history, limit its applicability to employer monitoring of employees' e-mail, the Act does contain three exceptions that often have the same practical effect. These exceptions are the provider exception, the ordinary course of business exception, and the consent exception.

The first exception to the ECPA prohibition on interception or accession of e-mail in the workplace is for e-mail service providers. Commentators have predicted that most private employers will be exempt from the ECPA under this exception if they provide their employees with e-mail service through a company-owned system. It is not as clear, however, whether the exception could be used to shield private employers who simply provide e-mail service to their employees through a third party internet service provider. A few recent court decisions have lent support to the proposition that the provider exception will exempt many private employers from liability under the ECPA. Thus, for private sector employees who use

---

27See 18 U.S.C. § 2510(12) (1994). See also Kopp, supra note 1, at 868 n.46 (noting that the ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photoptical system that affects interstate commerce").

28See Kopp, supra note 1, at 870-71 (citing 18 U.S.C. §§ 2511(2)(a)(i), 2511(2)(d), 2510(5)(a) (1994)).


32See 18 U.S.C. § 2511(2)(a)(i), which specifically authorizes:

[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 . . . .

33See Kopp, supra note 1, at 871 (explaining how the provider exception has been interpreted).

34Id.

35Id. at 872. The first court to apply the ECPA's provider exception in the context of workplace e-mail monitoring was the California Superior Court in Flanagan v. Epson America, No. BC007036 (Cal. Super. Ct. Mar. 12, 1991). The court found that there is no ECPA violation if the entity providing the e-mail service intentionally examined all the messages on the system. Id. Another court held that United Airlines, as a provider of its computer reservation system, was immune from liability under the Act after it monitored its reservations and discovered falsifications by a travel agent. The court concluded that under the provider exception, American Airlines was entitled to protect its rights and property. United States v. Mullins, 992 F.2d 1472 (9th Cir. 1992), cert. denied, 510 U.S. 994 (1993). See also Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (deciding that the employer, City of Reno, was the provider of the e-mail system within the meaning of the Act and that the provider exception "allows service providers to do as they wish when it comes to accessing communications in electronic storage").
a company-owned and provided e-mail system, any privacy in that e-mail is illusory.

The second exception under the ECPA is the ordinary course of business exception, or business extension exception.\footnote{See 18 U.S.C. § 2510(5)(a) (1994), which reads: [A]ny 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.} A prerequisite to a claim under the ECPA is that the alleged interceptor used an electronic device.\footnote{See 18 U.S.C. § 2510(4) (1994). This section provides that an interception can only occur through the use of an electronic or other mechanical device. See also Kopp, supra note 1, at 874 (discussing the statute).} The ordinary course of business exception is actually an exclusion from the definition of an electronic device.\footnote{See 18 U.S.C. § 2510(5) (1994).} This exception has not been applied to workplace e-mail, but based on its application in analogous contexts, such as telephone communications, it may well provide another shield for employers who engage in routine monitoring of their employees' e-mail.\footnote{Courts that have applied the ordinary course of business exception to telephone communications in the workplace have taken two approaches: the content approach and the context approach. The content approach permits an employer to monitor "business-related" communications but does not allow monitoring of personal communications. Conversely, the context approach looks to the employer's reason for monitoring its employees' communications to determine whether they had a legitimate business justification for the monitoring. See Kopp, supra note 1, at 874-75 (citing Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (holding that an employer cannot escape liability under the ordinary course of business exception for monitoring an employee's personal telephone call)). See also Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994) (holding that paltry evidence of bomb threats would not justify an employer's covert monitoring of employee telephone calls).} If employers can justify the monitoring of their employees' communications, whether via telephone or e-mail, with a legitimate business purpose, or limit their monitoring to business-related communications, they should escape liability under the ordinary course of business exception.\footnote{See Kopp, supra note 1, at 874.}

A legitimate business purpose would be to prevent unauthorized use of the telephone; therefore, an employer may intercept a call to determine whether the call is in fact a personal one.\footnote{See Watkins, 704 F.2d at 583 (holding that a personal phone call does not fall under the ordinary course of business exception, but may be monitored long enough to discern that it is personal).} Some courts, however, have not allowed a company who has surreptitiously monitored their employees' e-
mail to hide behind this exception. Therefore, the better course for employers is to inform their employees that routine monitoring will occur in order to further a company objective, such as quality control.

The third exception to the ECPA, with implications for the monitoring of workplace e-mail, is the consent exception. This exception generally applies when one party to the communication has given prior consent, actual or implied, to the interception or accession of the communication. Cases that have applied the consent exception in other contexts suggest that a published e-mail monitoring policy provided to all employees may allow employers to escape the ECPA prohibitions. If employees are informed of an affirmative monitoring policy with regard to their e-mail, and they still choose to use the e-mail system, they have effectively consented to the monitoring. Such consent is valid notwithstanding the fact that employees may be left with no other meaningful choice but to use the e-mail system. Many courts imply consent when an employee knew, or should have known, of an employer monitoring policy or if the employee used the business line to place a personal telephone call knowing the business line to be routinely monitored.

Other legislation aimed at providing greater protection to employees' use of workplace e-mail has been proposed by Congress but not yet adopted. The Privacy for Consumers and Workers Act was proposed in 1993, but did not materialize. It would have required employers to inform their employees of workplace monitoring and establish limits on the scope of the monitoring. The proposal also provided that information obtained in violation of its terms

---

42See Kopp, supra note 1, at 881 (citing Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994)).

43See id. at 882 (discussing the permissible scope of the consent exception).

44See Watkins, 704 F.2d at 583 ("[C]onsent . . . is not necessarily an all or nothing proposition."). See also Deal v. Spears, 980 F.2d 1153, 1155-56 (8th Cir. 1992) (rejecting the employer's consent defense because it had only warned the employee she might be monitored, not that she, in fact, would be monitored).


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 or laws of the United States or of any State.

Id.

46See Kopp, supra note 1, at 883 (citing Gantt, supra note 9, at 357-58).

47Consent may, however, be limited under these circumstances. For example, an employer who tells its employees that only business-related e-mail will be monitored will not be able to extend acceptance of that policy to include consent to monitor employees' personal e-mails. See Kopp, supra note 1, at 883.

48See Watkins, 704 F.2d at 581-82.
could not be used against any employee.\textsuperscript{49} One obvious reason this legislation was never passed is that companies and business advocates often lobby against such legislation as too burdensome.

States may enact legislation that is more protective of employee privacy rights than the ECPA.\textsuperscript{50} Some states have done just that.\textsuperscript{51} Also, many states have used the ECPA as a model for legislation, using provisions such as the prior consent and ordinary course of business-exception in their own statutes.\textsuperscript{52}

There is a lack of uniformity in state e-mail privacy laws. In states that have implemented more protective legislation, "such as those where the consent of 'all parties' is required, employers [may well] face limitations [on] monitoring employee communications."\textsuperscript{53} Legislation modeled after the ECPA, however, has done little for e-mail privacy rights,\textsuperscript{54} since state courts are interpreting the statutes as narrowly as the federal courts interpret the ECPA itself. Presently, privacy rights change from state to state and no state has passed a law specifically aimed at employee e-mail privacy rights.\textsuperscript{55}

C. Common Law Protection

Since both constitutional and statutory protection is limited with respect to an employee's right to privacy in workplace e-mail, many

\textsuperscript{49}See Kopp, supra note 1, at 883-84 (citing H.R. 1900, 103d Cong., 1st Sess. (1993)).

\textsuperscript{50}Courts have held that the ECPA will only preempt state law if the state law is less protective. See Rodriguez, supra note 2, at 1460 (citing United States v. McKinnon, 721 F.2d 19, 21 n.1 (1st Cir. 1983); Evans v. State, 314 S.E.2d 421, 425 (Ga. 1984), cert. denied, 469 U.S. 826 (1984)).

\textsuperscript{51}For example, legislation in California, Delaware, Florida, Illinois, Louisiana, Maryland, Massachusetts, Michigan, Montana, Oregon, Pennsylvania, and Washington requires prior consent by all parties before a communication may be intercepted. See Rodriguez, supra note 2, at 1461.

\textsuperscript{52}See Rodriguez, supra note 2, at 1461 n.149 (surveying several states' versions of the ECPA, including Arizona, Colorado, Delaware, Florida, Georgia, Hawaii, Kansas, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Texas, Utah, Virginia, West Virginia, Wisconsin, and Wyoming).


\textsuperscript{54}See Rodriguez, supra note 2, at 1461.

\textsuperscript{55}See id. Cf. 20 Okl. St. ch. 18, app. 3, Rule 7 (1999) (providing that e-mail sent over the electronic Oklahoma Court Information System is not private because other persons may be able to access and read the e-mail).
employees are turning to traditional state tort law actions.\textsuperscript{56} The tort of intrusion upon seclusion is most often cited as a basis for a claim by an employee against her employer for monitoring e-mail.\textsuperscript{57} This tort provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."\textsuperscript{58} Since this tort applies to invasions of privacy, both physical "or otherwise," it could be extended to protect against e-mail monitoring.\textsuperscript{59} Like the standard used in Fourth Amendment search and seizure analysis,\textsuperscript{60} the four elements of an intrusion upon seclusion claim are: (1) whether the intrusion was intentional,\textsuperscript{61} (2) whether the act in question would have been highly offensive to the average reasonable person,\textsuperscript{62} (3) whether the plaintiff's activity was subjectively and objectively private,\textsuperscript{63} and (4) whether the intruder had a legitimate purpose justifying the invasion.\textsuperscript{64}

\textsuperscript{56}See Kopp, supra note 1, at 884 (citing RESTATEMENT (SECOND) OF TORTS 652A (1977), that includes four separate torts which protect 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, and publicity that unreasonably places the other in a false light before the public).

\textsuperscript{57}See Kopp, supra note 1, at 884. In theory, this tort would apply when an employer intercepts, but does not disclose, an employee's e-mail messages. See Anne L. Lehman, E-Mail in the Workplace: Question of Privacy, Property or Principle?, 5 COMM. LAW CONSPECTUS 99, 104 (1997). When an employer discloses the contents of an employee's e-mail message, the employee may have a cause of action for the "unreasonable publicity given to another's private life" or, depending on the contents of the message, "publicity that unreasonably places the other in a false light." \textit{Id.}

\textsuperscript{58}RESTATEMENT (SECOND) OF TORTS 652B (1977).

\textsuperscript{59}See \textit{id.} at 652A. \textit{See also} Kopp, supra note 1, at 885.

\textsuperscript{60}The Fourth Amendment standard balances the employee's subjective and objective expectations of privacy against the employer's justification for monitoring." See Rodriguez, supra note 2, at 1463 n.165.

\textsuperscript{61}See \textit{id.} Courts have considered electronic surveillance, such as telephone "tapping," enough to establish this element of the tort. See \textit{generally} Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1991); Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. 1970); Marks v. Bell Tel. Co., 331 A.2d 424 (Pa. 1975); Billings v. Atkinson, 489 S.W.2d 858 (Tex. 1973).

\textsuperscript{62}See Rodriguez, supra note 2, at 1463 (citing RESTATEMENT (SECOND) OF TORTS 652B cmt. d (1965)).

\textsuperscript{63}In most instances, it is relatively easy to establish a subjective expectation of privacy. An employee, however, must also make a showing that their expectation of privacy was objectively reasonable, which is a much more difficult burden to carry. The burden could prove especially hard if the employer has issued a monitoring policy. \textit{See id.} (citing Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392 (W.D. Okla. 1982)).

\textsuperscript{64}See \textit{id.} at 1463 (citing Miller v. NBC, 232 Cal. Rptr. 668 (Cal. Ct. App. 1986); Horstman v. Newman, 291 S.W.2d 567 (Ky. Ct. App. 1956); Engman v. Southwestern Bell Tel. Co., 631 S.W.2d 98 (Mo. Ct. App. 1982)).
An employee bringing an intrusion upon seclusion claim based on the monitoring of e-mail should be able to show relatively easily that the intrusion was intentional. Similarly, an employee should be able to show a subjective expectation of privacy in her e-mail, especially if a password is required for access. The remaining elements, however, will not be quite as easy to establish. This is particularly true when the employer puts employees on notice that it might monitor the e-mail. Thus, courts may decide that the employer's conduct was not highly offensive, and the employee's expectation of privacy was not reasonable. Furthermore, courts have held that business interests can even justify activities that are extremely invasive. Some commentators argue that too much weight is given to business interests and that such preferential treatment minimizes workplace privacy interests. Therefore, even the intrusion upon seclusion tort, while providing some protection, does not favor the employee.

III. Analysis

Recent cases have applied the invasion of privacy tort to e-mail monitoring in the workplace. The first was a California case wherein the plaintiffs brought an action against their employer for intercepting and reviewing several personal e-mail messages. The court rejected the employees' claim for tortious invasion of privacy. It held that the employees did not have a reasonable expectation of privacy in their e-mail because they had signed a waiver form stating that e-mail use was limited to company

---

65 See id. E-mail monitoring will usually constitute an intentional act, unless the employer could show the invasion was incidental to system maintenance and therefore unintentional. See id. at 1463 n.170.

66 See Rodriguez, supra note 2, at 1463.

67 See id.

68 When employees are notified that they may be monitored, their consent to said monitoring can be implied. See Gantt, supra note 9, at 377. An employee may also have trouble proving that e-mail was actually read. See Marks v. Bell Tel. Co., 331 A.2d 424 (Pa. 1975) (holding that plaintiff failed to prove that the allegedly intercepted telephone conversations were actually heard by a third party).

69 See Rodriguez, supra note 2, at 1464 (citing Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382 (Mich. Ct. App. 1989) (holding that business interests justified home monitoring of an employee who claimed to have work-related injuries)).

70 See id. See also Gantt, supra note 9, at 377 (noting that the concept of "business interest" creates almost a legal safe haven for employers who choose to monitor employee e-mail messages" (quoting Jennifer Griffin, The Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee Privacy Rights, 4 SOFTWARE L.J. 493, 526-27 (1991))).


business. The court also noted that the employees were aware other co-workers, who were not the intended recipients of the messages, had read their "private" e-mail messages in the past. The fact that employees received personal passwords to access the e-mail system and were explicitly told to safeguard those passwords did not, in and of itself, establish a subjective expectation of privacy.

A Pennsylvania District Court case also addressed the claim of tortious invasion of privacy by an employee against his employer for reading his e-mail. The employee brought a suit against his employer for wrongful discharge after being fired when company executives read the contents of e-mail messages he had sent to his supervisor which contained derogatory remarks about the company and management personnel. In that case, the court refused to find a reasonable expectation of privacy in e-mail communications voluntarily made by the employee to his supervisor over the company e-mail system, notwithstanding, the many assurances given by the company that e-mail communication would not be intercepted or read by management.

Furthermore, once the employee had transmitted the e-mail to a second person over an e-mail system that was utilized by the entire company, any reasonable expectation of privacy was lost. The court contrasted these facts against much more intrusive employment practices, such as requiring employees to submit to urinanalysis and personal property searches, which have been condoned by courts. In so noting, the court suggested those cases pose a much closer invasion of privacy question. With e-mail monitoring, employees communicate via the e-mail system voluntarily and they are not forced to disclose any personal information. Furthermore, the court found that even if an employee has a reasonable expectation of privacy in the contents of e-mail sent over the company e-mail system, the company's interception of the e-mail is not "a substantial or highly offensive invasion of privacy." In short, "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system

73 Id. See also Kopp, supra note 1, at 885 (discussing Bourke).
75 Id.
77 Id. at 98-99.
78 Id. at 101.
79 Id.
81 Id.
outweighs any privacy interest the employee may have [had] in those communications."\(^{82}\)

A similar result was reached in an analogous Massachusetts case.\(^{83}\) The employer in that case provided an e-mail system for its employees, supplied them each with a password, encouraged them to change their passwords periodically, and did not have a policy against using e-mail for personal messages.\(^{84}\) Although supervisors had access to employees' computer files, including e-mail, and those files were routinely saved onto back-up files to which supervisors also had access, employees were not told of the possibility that their e-mail could or would be monitored.\(^{85}\) Inevitably, a disagreement arose between some employees and management. After a report that one of those employees was spending excessive amounts of time on the e-mail system, the manager accessed his personal e-mail files and found many messages disparaging the state wiretap law and invasion of privacy. The Massachusetts law,\(^{87}\) similar to the ECPA, included an ordinary course of business exception that the court found immunized the employer from liability.\(^{88}\) The court, however, refused to grant the employer's motion for summary judgment on the invasion of privacy claim stating that it remained to be seen whether the employees had a reasonable expectation of privacy in their e-mail.\(^{89}\)

Another case out of Texas also rejected an employee's claim of invasion of privacy arising from the employer reading personal e-mail.\(^{90}\) The court held that the e-mail messages contained on the company computer

---

\(^{82}\)Id.


\(^{84}\)Id. at *2. The employer did, however, have a policy against "excessive chatting" via e-mail. \(\textit{Id.}\)

\(^{85}\)Id.

\(^{86}\)Id. at *3. The manager spent eight hours reading over employees' e-mail that had been saved in a back-up system. He found e-mail between two employees in particular that included negative references to himself. \(\textit{Id.}\)


\(^{88}\)Restuccia, 1996 Mass. Super. LEXIS 367, at *2-*3. The court found that a back-up system which automatically stored employee e-mail messages was the "type of permissible interception contemplated by the ordinary course of business exception." The court rejected employees' argument that the unlawful interception was the reading of the e-mail and not the back-up system itself. \(\textit{Id.}\) at *5.

\(^{89}\)Id. at *9. The employees will have to show not only that they had a reasonable expectation of privacy, but that the manager's "reading of the E-mail messages constituted an unreasonable, substantial or serious interference with [their] privacy." \(\textit{Id.}\)

were not an employee's personal property but were "merely an inherent part of the office equipment." 91 The court noted that workstations were provided by the employer so that employees could perform the functions of their job, and the workstations happened to include a computer and e-mail system. 92 The fact employees had passwords carried little weight because e-mail was first sent over the network where it was accessible by third-parties. 93 Finally, the court held that even if the employee had an expectation of privacy in his e-mail, that expectation would be outweighed by the company's interest in preventing inappropriate and unprofessional comments, as well as illegal activity, over its e-mail system. 94

A few employee e-mail cases have arisen in which United States servicemen brought suits against the government, as their employer, claiming invasion of privacy as well as violations of the Fourth Amendment and ECPA. 95 As with the private sector cases, the employees' claims have failed after the court determined they had no reasonable expectation of privacy in e-mail sent over the system supplied by their employer — the federal government. 96

All of the previously discussed cases bolster a company's right to monitor workplace e-mail: holding that maintaining a personal password to access the e-mail system is not like a key and does not give rise to an objectively reasonable expectation of privacy, 97 and that even when an employer's stated policy privatizes employee e-mail, an objectively reasonable expectation of privacy does not follow. 98 They all seem to be in agreement that employees do not have a reasonable expectation of privacy in their workplace e-mail. If these cases prove to be the norm, future common law will also be interpreted to favor employers. 99

---

91 Id. at *11.
92 Id.
93 Id. at *13.
95 See United States v. Monroe, 50 M.J. 550 (A.F.C.M.R. 1999), aff'd, 52 M.J. 326 (C.A.A.F. 2000) (recognizing that "the existence of a personal password is only of passing significance," because the password was not issued to exclude the system administrator and the plaintiff was on notice that the e-mail system was supplied by the government and subject to its control).
96 Id. at *22. See also United States v. Simons, No. 99-4238, 2000 U.S. App. LEXIS 2877, at *11 (4th Cir. Feb. 28, 2000) (holding that the government's policy put the employee on notice that it would "audit, inspect, and/or monitor" employees use of the Internet and e-mail so that the employee could not argue he had a reasonable expectation of privacy).
99 See Kopp, supra note 1, at 886.
The varying causes of action discussed above exemplify the difficulty of proving an invasion of privacy claim against an employer for monitoring employee e-mail.\textsuperscript{100} The United States Constitution and several state constitutions offer some privacy protection to public employees, but private employees must rely on legislation or common law tort actions.\textsuperscript{101} The ECPA is ill-equipped to handle employee claims of invasion of privacy against their employers for e-mail monitoring, and courts that have examined the problem seem unwilling to recognize any privacy in employee e-mail communications.\textsuperscript{102}

There does still exist a possibility that an employer may be found liable for e-mail monitoring under the ECPA.\textsuperscript{103} If, for example, the employer provided e-mail service to its employees through a common carrier and did not maintain an e-mail consent policy governing employee usage of the e-mail service, there may well be a violation of the ECPA for intercepting employee e-mail.\textsuperscript{104} The use of a common carrier should overcome the provider exception, and the lack of a written policy should negate the consent exception. The only remaining hurdle for the employee would be the ordinary course of business exception. Even this exception could be negated, if the employee could show that the employer monitored purely personal e-mail communications and could not articulate any legitimate business interest in doing so.\textsuperscript{105}

IV. Evaluation

Although the ECPA was enacted to protect certain electronic communications from unauthorized access or interception, its main concern was overzealous law enforcement.\textsuperscript{106} Accordingly, both the ECPA and the cases on point allow a written e-mail policy to immunize the employer from liability if the employer does not act in contravention of that written policy.\textsuperscript{107} Thus, employers can virtually "write their own laws" on the

\textsuperscript{100}See id. at 886-87.
\textsuperscript{101}Id. at 887.
\textsuperscript{102}Id.
\textsuperscript{103}See Kopp, supra note 1, at 887.
\textsuperscript{104}Id.

\textsuperscript{105}Id. at 888. The ordinary course of business exception would also fail as a defense for an employer who monitored employee e-mail in contravention of a written e-mail policy. See id.

\textsuperscript{106}See United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999). Although it provides some degree of privacy, "the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of reasonably objective for Fourth Amendment purposes. Despite its concern for privacy, Congress did not provide for suppression where a party [violates] the Act." Id.

\textsuperscript{107}See Kopp, supra note 1, at 888.
subject by initiating a written e-mail policy that is distributed to all employees.\textsuperscript{108}

Given the current state of the law, and with no indication that it will change in the near future, employees need to be aware of their lack of privacy rights in workplace e-mail. With the broad power courts have given companies to monitor the e-mail of their employees, it does not seem likely that those companies will voluntarily impose limits on their own power. After all, it is in a company's best interests to simply provide a written e-mail policy to its employees that informs them that their e-mail is the property of the company and that they have no privacy interest in it whatsoever. To ensure that companies' policies are being followed, employers can monitor any employee's e-mail at any time.\textsuperscript{109} Programming a banner at the top of the e-mail portal reminding employees that the e-mail they send and receive is

\textsuperscript{108}Id. An example of a company e-mail policy is:

**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, intimidating, 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 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.

Id. at 888-89 n.204 (quoting Robert P. Fitzpatrick, Technology Advances in the Information Age: Effects on Workplace Privacy Issues, SC08 ALI-ABA 599, 625 (July 17, 1997)).

\textsuperscript{109}Id.
the property of the employer and subject to its supervision would also contribute to destroying any claim of privacy an employee might have.\footnote{See United States v. Monroe, 50 M.J. 550, 555 (A.F.C.M.R. 1999) (noting that government system contains banner warning that "USERS LOGGING ON TO THIS SYSTEM CONSENT TO MONITORING"), aff'd, 52 M.J. 326 (C.A.A.F. 2000).}

Companies do (and rightly should) have a strong interest in the contents of employee e-mail. The company provides e-mail service to its employees not so they can keep in touch with long-distance acquaintances, but rather to facilitate the work that needs to be done for the employer.

More serious abuses of company provided e-mail can expose the company to liability. For example, many aggrieved employees have found that e-mail messages sent around the office can be persuasive evidence of discrimination or sexual harassment.\footnote{See Samuel A. Thumma & Darrel S. Jackson, The History of Electronic Mail in Litigation, 16 COMPUTER & HIGH TECH. L.J. 1, 14-15 (1999) (noting many cases where a racist or sexist e-mail has been relevant to a discrimination claim).} Sexually explicit or racially discriminatory jokes or pictures e-mailed from one employee to another in the office could well provide the basis for a claim of sexual harassment or discrimination, that could expose the employer to liability for allowing a hostile work environment.\footnote{See id. at 15. See also Vicarelli v. Business Int'l, Inc., 973 F. Supp. 241, 242 (D. Mass. 1997) (invoking a suit against a company after supervisor sent sexually explicit e-mails to employee's home).} Furthermore, inter-office e-mail is often held by courts to be discoverable material.\footnote{See Thumma & Jackson, supra note 111, at 8-10 (citing cases where companies have not only been forced to produce all inter-office e-mail communications for purposes of litigation but also bear the cost of its retrieval from databases). One court held that e-mail records were entitled to the same protection as paper records under the Federal Records Act and thus the government could not destroy them. See id. at 7-8 (citing Armstrong v. Executive Office of the President, 1 F.3d 1274, 1285-87 (D.C. Cir. 1993)).} Just as companies are forced to disclose inter-office memos in the course of litigation, so too may they be forced to provide the contents of their databases.\footnote{See Thumma & Jackson, supra note 111, at 8-10.} Therefore, it is important that companies have control over the workplace environment.

With this in mind, educating employees about company e-mail policies is the best way to address privacy concerns. Proper education will ensure that employees are informed and aware that the e-mails they send or receive at work are not private. If this is made clear to employees, their subjective expectations of privacy will vanish, as will failed attempts to hold companies liable for monitoring employee e-mail communications. Moreover, employee education is needed so that employees do not use their workplace e-mail to send personal or private messages.

If an employee does wish to safeguard her workplace e-mail, technological options, such as anonymous remailers and encryption, are
needed the available. An anonymous remailer is "a service to which a message is initially sent that strips away all identifying information before forwarding the message to the intended recipient." Although it carries with it some problems of its own, use of anonymous remailers could provide some needed privacy to employees' workplace e-mail.

Encryption programs are a bit more sophisticated but offer greater protection to one's e-mail message. Specifically, encryption software "allows users to transmit secure e-mail messages which only the intended recipient can decode by use of a 'decryption key.'" The most commonly used encryption is "public-key cryptography." This process requires that both the sender and the recipient use a cryptography program to create two passwords, or "keys." The user retains one password as a "private" key, while the other key is "public," to be distributed to those people from whom the user wants to receive encrypted messages. "Only the private key can decrypt messages encoded with the public key." Encryption technology, however, is much more involved than the average employee using workplace e-mail is likely to be familiar with. Therefore, while it does offer a valuable means of protecting one's workplace e-mail, its wide-spread use is unlikely. Even if encryption were to become more mainstream, employers could retaliate against the loss of control by prohibiting the use of encryption on company e-mail.

Encryption techniques are currently under fire by the United States government. Law enforcement officials fear encryption will allow criminals, both domestic and abroad, to communicate and coordinate illegal activity. Accordingly, the government wants to require all encryption programs to permit "lawful access" whereby law enforcement officials, with

---

115 See Rodriguez, supra note 2, at 1472.
116 Id. at 1470.
117 See id. (noting that anonymous remailers can facilitate "fraudulent electronic commerce, harassment, and defamation"). These concerns have prompted commentators to call for legislation that would "eliminate liability for network providers if they are willing to disclose the identities of anonymous users who utilize the network to coordinate or conduct illegal activities." Id. at 1470-71 (citations omitted).
118 See id. at 1471-72.
119 Rodriguez, supra note 2, at 1471.
120 Id.
121 Id.
122 Id.
123 Rodriguez, supra note 2, at 1471.
125 See id.
a valid search warrant, could access the encrypted information. Although this controversy at first seems to have little relevance here, an approach similar to the one the government is taking may be adopted by companies if use of anonymous remailers and encryption were to become more common in the workplace. If many employees begin using these techniques to protect their workplace e-mail from the prying eyes of their employers, companies are sure to rebel against the loss of control. As legislatures and courts have been generally reluctant to allow invasion of privacy claims against employers for monitoring workplace e-mail, they will likely be receptive to company actions to secure their e-mail systems. Businesses are certainly entitled to control their workplace, especially where widespread use of encryption techniques could attack their control and leave the employer open to liability.

V. CONCLUSION

At this time, the law seems to favor businesses and allows their interest in controlling the workplace to outweigh an employee's privacy interest in personal e-mail. Constitutional guarantees, both federal and state, offer little protection, and then, only to public employees. Likewise, federal and state regulations have been consistently interpreted by courts across the country in favor of businesses. The same trend is apparent when employees attempt to bring common law tort claims for invasion of privacy against their employer. Corporations can protect themselves from employees' invasion of privacy claims simply by establishing a clear written policy on workplace e-mail monitoring. If employees make an effort to understand the policy of their employer with respect to e-mail monitoring, they will be less likely to transmit e-mail from work that would be disapproved of by their employer. Employees need to take responsibility for their own privacy rights and protect those rights by not using workplace e-mail for private messages. Finally, for the more computer-literate employees, technology is available that could help bring a level of privacy to e-mail, even at work. Businesses,

---

126 id.


128 See Rodriguez, supra note 2, at 1472 (citing Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994) (noting that an "entire network may be confiscated if law enforcement learns of encrypted criminal activity on a private network").
however, will not likely allow such usurpation of control in their company e-mail, and courts may well come out on their side.

Sarah DiLuzio