Each morning, you arrive at work and turn on your personal computer. While the computer beeps and changes screens, checking for viruses and verifying that all is well in your computer world, you pick up a stack of papers and begin to review your mail. As you open and read the material, the thought that someone else has already read this mail never enters your mind. Of course not. It's your mail. It's personal and private. Not only would it be rude for someone to read your mail, it is illegal. Satisfied that you have not missed important deadlines, you turn again to your computer, enter your user identification number, enter your password, and decide to check your e-mail. Same thing, right? It's mail, sent to your personal electronic address, and protected by a password. It's personal, private, and it would be rude for someone else to read it. Unfortunately, reading employee e-mail, from a different computer terminal and without your consent, is technologically possible, entirely legal, and routinely practiced by employers to monitor their employees. Even those messages that have been "deleted" or "trashed" might not escape the eye of the employer.

A survey of 301 companies in 1993 revealed that at least twenty-one percent searched employees' computer files, voice mail, and e-mail or other networking communications systems. In addition, almost one-third of these companies did not warn their employees of this practice. A 1996 study on workplace privacy by the American Civil Liberties Union estimates that 20 million employees have their e-mail, computer files and voice mail searched by their employers. Consequently, many employees are unaware of either the capability, or the willingness, of employers to monitor employees through their computers. Meanwhile, employer incentive to monitor employees through the use of computers is enhanced by the ease and capability provided by advanced technology. The motivation to monitor employees is further compounded by the potential liability that employer's face for the contents of employee e-mail messages and employee activities on the Internet. Such actions are justified by the argument that the computer system is owned and operated by the company, and that the employee is on the job performing tasks related to the job. The unhappy consequence is a situation wherein the employee's privacy rights are routinely invaded by the employer, who, at the same time, ar-

---

1. Charles Piller, Bosses With X-ray Eyes, MACWORLD, July 1993, at 118, 120. The study additionally revealed, that when the number of employees in a company reaches 1,000 employees, the percentage of respondents indicating that they search employee files rises to thirty percent. Id.
2. Id. at 122.
6. See, e.g., Meloff v. New York Life Ins. Co., 51 F.3d 372 (2d Cir. 1995) (allowing employment discrimination and defamation claims to proceed, where employer sent notification of plaintiff's termination to individuals in the company on the electronic mail system, and where employer sent a company-wide message entitled "Fraud" which asserted plaintiff defrauded the company); Boone v. Federal Express Corp., 841 F. Supp. 1186 (S.D.N.Y. 1995) (finding sufficient evidence to defeat motion for summary judgment in a sexual discrimination case, in which evidence included e-mail messages sent by Microsoft employees to plaintiff and other employees was provided).
guages that he or she is only exercising legitimate and protective rights as an employer.9

These positions become darkly adversarial when the monitoring of personal e-mail accounts results in the termination of an employee, or some other disciplinary action. Not surprisingly, employees are increasingly looking to Congress for some recognition of and protection from this invasion of privacy. Others are looking to the courts to develop a framework which suitably and fairly addresses these competing interests.

Responding to these interests, in August 1996, a California based group known as Cyberspace Professionals for Social Responsibility (CPSR),9 issued a statement of "Electronic Privacy Principles"10 containing guidelines for employer providers, service providers, and other groups that have access to personal information about their subscribers or users. The document calls for united efforts on the part of service providers and employers to protect the privacy of those using their services.11 The paper urges employers to provide and follow clear company policies delineating acceptable uses of e-mail, describing the procedures which will be used for enforcing the policy, and outlining penalties to be imposed for improper use of the system.12 Users are also encouraged to become aware of their employer's policy and the risks of using computer and e-mail networks.13 These proposals, however, have not been solidified by federal legislation or by court decisions, and any effect the policies may have in litigation is still uncertain.

In light of the importance of developing law appropriate in this area, this Comment evaluates and explains the direction the courts have recently taken. Part I discusses the types of law which may provide protection of employee e-mail, and which may aid the courts in developing a framework of analysis. Part II addresses recent cases in which courts have allowed employer access of the employee's e-mail and rejected claims of invasion of privacy. Part III examines the rationales of these cases and suggests that the court decisions provide inadequate protection from unwarranted invasions of privacy and run counter to public concern. Part IV proposes that, in order to balance the important interests of employees' privacy and employer's rights as providers of the network, guidelines should be established which diminish the likelihood that companies will be held liable for the unauthorized activities of their employees, thus reducing the incentive to monitor and control the e-mail of employees. This alleviation of liability, coupled with the development of responsible and balanced company policies, will diminish the intrusion into employee e-mail.

I. SOURCES OF PROTECTION FROM EMPLOYER MONITORING OF EMPLOYEE E-MAIL

A. The United States and State Constitutions

The Fourth Amendment provides the general right of privacy in the United States Constitution.14 It is settled, however, that the Fourth Amendment protects people from unreasonable searches and seizures performed by the government, and does not necessarily apply to searches

8 Id. Hal Coxson, a management lawyer, lists other justifications for employer monitoring of employees. According to Coxson, legitimate business reasons for the monitoring include: (1) monitoring employee performance, which includes monitoring productivity, quality of work and customer satisfaction; (2) detecting employee misconduct, specifically, theft, drugs, gambling, misuse of company property for disclosure of confidential material over e-mail; (3) protecting employees' safety and health; (4) reducing liability for employee acts. Mr. Coxson notes that employees are capable of gaining access to sexually explicit material over the World Wide Web, which can create a hostile work environment, for which the employer can be held liable. Increased monitoring of employee's use of their computers and software is therefore justified. Id.


10 Id. at 1.

11 Id. at 2.

12 Id. at 1.

13 The Fourth Amendment to the U.S. Constitution provides that the "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. While the amendment does not explicitly protect or articulate a right of privacy, the Supreme Court has found it to fall within the ambit of the amendment. See Griswold v. Connecticut, 381 U.S. 479, 485 (1965).
performed by private parties.\textsuperscript{15} Therefore, unless a person is employed by the government, the Fourth Amendment does not offer a protection of privacy in that employee's e-mail.

Many state constitutions also contain either an explicit right to privacy or have been read by the courts of the state to protect the right of privacy. While most rights of privacy, like those in the U.S. Constitution, protect the individual from government intrusion into this right, there appears to be a trend toward providing a right of privacy which extends to the workplace for those employed in the private sector.\textsuperscript{16} California's protection, for example, has been interpreted to prohibit infringements into privacy unless the invasion is justified by a "compelling interest."\textsuperscript{17} It is not clear, however, whether the broad protection of privacy which states have granted will be extended to private sector employees regarding their e-mail messages in the face of competing arguments for the right of the employer to monitor the employee use of the service.

\begin{itemize}
\item \textsuperscript{15} See, e.g., United States v. Jacobsen, 466 U.S. 109, 113-14 (1984) (stating that a search or seizure performed by a private individual, "even an unreasonable one," is not proscribed by the Fourth Amendment); see also Paul F. Gerhart, Employee Privacy Rights in the United States, 17 COMP. L.A.R. 175, 176 (1995) (noting that Constitutional protections of government employees "do not extend to citizens vis-à-vis each other," and that therefore, "public sector employees enjoy greater explicit protection of their privacy rights than private sector employees do"); Laurie Thomas Lee, Watch your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop," 28 J. MARSHALL L. REV. 139, 146 n.37 (1994) (observing that since "only government employees may claim a Constitutional privacy right should their e-mail be accessed; nongovernment employees have no Constitutional guarantee of privacy in the workplace, unless infringed by a government search or seizure[,]"") employees in the private sector "actually enjoy less privacy protection than those working for the government").
\item \textsuperscript{16} See, e.g., 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 enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy"); see also Lee, supra note 15, at 149-50, 173 (outlining state constitutional protections and the corresponding interpretations of the state courts).
\item \textsuperscript{17} See CAL. CONST. art. I, § 1; see, e.g., Porten v. Univ. of San Francisco, 134 Cal. Rptr. 839 (1976) (finding improper the disclosure of a student's grades by a private university to the State Scholarship and Loan Commission); White v. Davis, 120 Cal. Rptr. 94 (1975) (stating that the amendment to the
\end{itemize}

B. Federal Statutes

Federal statutes appear more likely to offer protection for the privacy of e-mail in the workplace. The Electronic Communications Privacy Act of 1986 ("ECPA") is the primary statute in this area.\textsuperscript{18} The ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Street Act of 1968,\textsuperscript{19} and was passed in recognition of the need to update privacy protection in order to remain abreast of quickly changing and developing technology.\textsuperscript{20}

Generally, the ECPA amended the federal wire-tap statute by adding the protection of "electronic communications" wherever the act had previously protected wire and oral communications,\textsuperscript{21} and prohibits the interception of these communications.\textsuperscript{22} The disclosure and dissemination of information obtained in violation of the statute is also prohibited.\textsuperscript{23} Additionally, while the transmission of communications is protected from interception by § 2511 of the Act, a provision was


23 18 U.S.C. § 2511(c) - (d) (1994).
also included to protect the electronic storage of the communications.24

Although the legislative history of the ECPA indicates that e-mail was intended to fall within the ambit of the Act's protection25 there are provisions and exceptions which limit that protection and which, in reality, permit employers in a private company to access the e-mail of their employees without violating the statute. Generally, the statutory language creates an "ordinary course of business" exception, an exception under the stored communications provisions, a limitation under the commerce clause, and an exception based on consent.26

First, the ECPA retains language which establishes an "ordinary course of business" exception. The definition of "device" specifically excludes any telephone or component "furnished to the subscriber or user by a provider of [the . . . ] communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business . . . ."27 It is unclear from this definition whether a modem, software, or the specific computer system or organization used by the network manager will be considered an interception device by the courts. If these components are excluded from the definition of device, interception of e-mail would be permitted by this provision.28 Private telephone networks are clearly covered by the business use exception, which allows employers to monitor employee telephone calls with little risk of liability.29 Additionally, because the ECPA contains a similar provision that is broader in scope than the telephone device exception but is not limited to specific types of equipment, it may be read to include private company networks.30 This section states that it is not unlawful for an:

operator of a switchboard, or 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 . . . .31

Although "provider" is not defined in the statute, it could be interpreted to be the owner and operator of a private network — such as within a company.32 Further, where the "provider" is seen

24 See 18 U.S.C. § 2701 (1994). The statute makes subject to punishment whoever "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a) (1994). "Electronic Storage" is defined in § 2510(17) as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (1994).

25 S. REP. No. 541, 99th Cong., 2d Sess., at 14 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568, reviewed by Lee, supra note 15, at 151 (observing that although the ECPA does not specifically mention electronic mail, it is included in the scope of the general provisions, as is indicated by the prohibition of interception of electronic communications, which, according to the legislative history includes e-mail); see also Thomas R. Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 AM. U. L. REV. 219, 236 (1994).


27 18 U.S.C. § 2510(5)(a)(i) (1994). This section defines device as:

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


29 See, e.g., Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994) (applying provisions of the ECPA where a company recorded telephone conversations of an employee);Deal v. Spears, 980 F.2d 1155 (8th Cir. 1993) (applying provisions of the ECPA where telephone conversations were intercepted and recorded); Briggs v. American Air Filter Co., Inc., 630 F.2d 414 (5th Cir. 1980) (interpreting the "extension telephone exception" of the ECPA); see Greenberg, supra note 25, at 235-36.

30 18 U.S.C. § 2511(2)(a)(i) (1994). This section limits the access of a provider of wire transmission service to the public in that such provider is not permitted to use random monitoring except for service or mechanical control checks. Id. The same limitation is not placed on the provider of the electronic communication because it was believed that total access is necessary to ensure proper function of the service. Greenberg, supra note 25, at 237 n.97.


32 See Greenberg, supra note 25, at 236 n.91 (noting that the language of the section was changed from "any communication common carrier" to "a provider of wire or electronic communication service" and suggesting that the section envisages the right to intercept the communications if the employee of a business with a private communications system intercepts another employee's message in the normal course of the employee's employment and it occurs as a result of
as a large public network, the company could be a “subscriber” or an “agent” of the “provider,” and thus fall under the exception.

Should the reading of service provider as owner of a private network, or as agent to the provider, prevail, the door is opened to monitoring by the employer through a second exception under the stored communication provisions. According to the provision, it is lawful to access stored communications if it is done pursuant to authorization “by the person or entity providing a wire or electronic communications service.” Therefore, if a company that supplies e-mail service to its employees is seen as a service provider, simple authorization from the company is required to access the stored messages received and sent by its employees. The employer or service provider would, however, be required to prove the monitoring was carried out in the ordinary course of business and necessary to the performance of the service or to protect rights or property. Courts may find the mere need to prevent abuse of the system and computer crime reason enough to allow system monitoring. Thus, the ECPA would permit the employer to monitor its employee’s e-mail.

Still other aspects of the Act are seen as providing exceptions to the general prohibition of monitoring. For example, since the jurisdiction of Congress is limited to interstate commerce, the definition of “electronic communications” under the ECPA is limited to communications and systems which “affect interstate or foreign commerce.” Consequently, a small intracompany system which does not cross state lines may not be covered by the ECPA. Additionally, under the ECPA interception of communications is permitted where one of the parties to a communication has given prior consent. Therefore, whether or not personal employee communications are protected may depend on the notion of implied consent. To determine the existence of consent, the court may consider whether the company has a policy on e-mail in the workplace, whether the employee is aware of the policy and whether the employee has agreed to abide by that policy. In this respect, the presence of a policy could work against the employee’s claim of privacy if the policy addressed the possibility of monitoring. The company would not, however, be permitted to go beyond the parameters of the policy.

C. State Statutes

Many states also have statutes which limit the interception of electronic communications. Although states are free to enact measures which restrict employer monitoring of employees further than the federal statute, many of the states which have statutes simply incorporate the ECPA exceptions pertaining to consent and business use. Study of the particular state statutory framework is necessary to determine the scope of protection provided by the statute because, for example, while the “business use” exemption may apply only to “common carriers,” a “prior consent” provision in the statute may still enable the employer to access the employee’s e-mail messages without violating the statute. Furthermore, while most states have wiretapping statutes which may offer protection from employer wiretapping for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce . . . .

35 Lee, supra note 15, at 155 (suggesting that “provider” will likely include public e-mail networks, such as Prodigy and CompuServe, and could include companies with their own e-mail systems on their own interstate area). It should further be noted that the statute specifically addresses “a person or entity providing an electronic communication service to the public,” prohibiting this provider from intentionally divulging the contents of any communication while in transmission on the service. 18 U.S.C. § 2511(3)(a) (1994). This may suggest a distinction in the definition of “providers,” and, thus, support the reading of “provider” as a private company.

36 See Lee, supra note 15, at 155.


40 See Greenberg, supra note 25, at 222-24 n.16 (listing state statutes which provide a private right of action for illegal wiretapping).

41 See Lee, supra note 15, at 175 (outlining state statutes with prior consent and business use wiretap exemptions – Table 2).

42 See Lee, supra note 15, at 158-59 (discussing state statute protection and noting that although some states require the consent of “all parties" this requirement may not necessarily provide greater protection if the message in question is an intracompany message, for a company policy on the issue, or an employee/employer relationship may be found to constitute implied consent).
tapping and interception of communications, other states are more permissive and specifically allow the monitoring.

Efforts at the state level to restrict employer monitoring of employee e-mail have been largely unsuccessful. Despite the failure to restrict monitoring, some state legislatures are making efforts to require employers to inform employees of potential monitoring of employee e-mail. For example, in 1996 the Colorado legislature proposed a bill that would require the employer to develop a policy regarding the privacy of electronic mail and to inform employees of the policy.

D. New Legislation

Attempts at the federal level to restrict employer monitoring of employee e-mail have met similar difficulties. The Telecommunications Act of 1996 did not address the issue of employer monitoring or accessing the e-mail messages of employees. The Privacy for Consumers and Workers Act does, however, represent an effort on the part of the federal government to protect employees from intrusions in the workplace by the employer. The proposed law would limit the employer's ability to monitor employees by requiring an explanation to new employees as to how they will be monitored, and how the information gathered would be used. Furthermore, it would require notification by the employer before the monitoring occurs and it would place a cap on the total time the employer would be permitted to monitor the employee. Moreover, the bill provides an important caveat; the employer may not act in regard to the employee based on information illegally obtained.

Although the bill has gained support, it has also been the subject of much debate. Opponents point to vague and undefined terms, claiming the bill will be difficult to administer and unnecessarily burdensome. Others argue that the limits would hinder the growth of the electronic messaging business. Thus, although the bill demonstrates the recognition of the problem, it also represents the inherent obstacles in creating a solution.

E. The Common Law

Still another source of protection lies in a common law suit for invasion of privacy. Under the tort of invasion of privacy, "intrusion into seclusion or private affairs" applies most aptly in the context of e-mail in the workplace. This tort is committed by "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." Courts will consider several factors to ascertain whether a person's privacy has been infringed to merit recovery. Courts generally will evaluate: (1) whether there was an intentional intrusion; (2) the location and private nature of the activity involved; (3) whether the intrusion was "highly offensive to the reasonable person;" and (4) whether the infringer had a legitimate purpose warranting the intrusion. Relatively few cases have dealt with this tort in the context of e-mail and invasion of privacy by an employer. Consequently, analysis of these issues has focused largely on the issue, and an indication that it is far from settled, is the introduction of the Telephone Privacy Act of 1993 which would make it lawful to intercept electronic communication where "such person is an employer or its agent engaged in lawful electronic monitoring of its employees' communications made in the course of the employees' duties." Telephone Privacy Act of 1993, S. 311, 103d Cong. § 2.


As an indication of the polarity of positions taken on
on how courts would approach a claim under this tort, and the various analogies which could be made to current and established case law. The success of this claim as applied to e-mail in the context of the workplace will be fact-specific. Therefore, in order to determine such issues as the employee's expectation of privacy in the electronic message system, which is a consideration necessary for the determination of whether the intrusion is "highly offensive," the court will have to consider such factors as whether the company had a policy in place regarding the use of the e-mail system. If the company has a policy, and the employee is informed of potential monitoring, the expectation of privacy may be reduced. The result, then, is that even under the common law tort of invasion of privacy, the employee's right to the privacy of her or his e-mail is not protected.

II. CASE LAW AS FURTHER POLARIZATION OF THE POSITIONS

Electronic mail has spurred the development of law around problems and issues which have never before been addressed. For example, hard copies of electronic mail messages have been introduced into evidence in courts as proof of harassment. Only recently, however, courts have begun to address the problem on its face: are e-mail messages sent by an employee to another person, fellow employee or not, entitled to protection from invasion by the employer?

The cases are beginning to be heard, testing the protection offered by the Fourth Amendment, the ECPA, and common law suit of invasion of privacy. The results, however, only aggravate the problem.

A. Smyth v. Pillsbury Company

The common law claim of invasion of privacy was addressed in Smyth v. Pillsbury Company. In Smyth, a regional operations manager for The Pillsbury Company ("Pillsbury"), an at-will employee, brought suit against his employer for wrongful discharge. The District Court for the Eastern District of Pennsylvania dismissed the action, finding that Pillsbury did not tortiously invade Smyth's privacy when it intercepted his e-mail, and, therefore, that it did not violate public policy when it terminated his employment based on the contents of the messages.

Smyth was discharged in 1995 for communicating what the defendant considered to be "inappropriate and unprofessional comments" over the defendant's internal e-mail system. Smyth's messages were part of a series of messages exchanged between Smyth and his supervisor. Initially, Smyth was responding to messages received on his computer at home from his supervisor in the company. The termination was directly contrary to the company's policy on e-mail, which assured the employees of Pillsbury that "all e-mail communications would remain confidential and privileged" and that "e-mail communications could not be intercepted and used by [Pillsbury] against its employees as grounds for termination or reprimand."

Smyth attempted to establish his claim of wrongful discharge on the basis of invasion of privacy. He argued that "public policy precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law." In particular, Smyth relied on the Pennsylvania Court of Appeals opinion in Borse v. Piece Goods Shop, Inc. In Borse, the Court of Appeals considered a claim for wrongful discharge where the plaintiff was fired after refusing to submit to urinalysis screening and personal property searches at her work-

---

56 See generally, Lee, supra note 15, at 162-64 (explaining and outlining the parameters and requirements of the tort based on cases involving eavesdropping on the telephone, photographing of employees, searching employees desks and lockers, opening of personal mail, and recording conversations).
57 See e.g., Knox v. Ind., 93 F.3d 1327 (7th Cir. 1996).
59 Id. at 98.
60 Id. at 101.
61 Id. at 98.
62 Id. at 98. The opinion does not reproduce the contents of the messages received by Smyth, but notes Defendant's allegation that Smyth's e-mails "concerned sales management and contained threats to 'kill the backstabbing bastards' and referred to the planned Holiday party as the 'Jim Jones Koolaid affair.'" Id.
63 Smyth, 914 F. Supp. at 98.
64 Id.
65 Id. at 100.
66 Id.
Although the court in Borse declined to find the company's procedure in violation of public policy, it opened the door to a wrongful discharge claim based on invasion of privacy by noting "other evidence of a public policy" may give rise to such a claim. 69

The Court of Appeals in Borse outlined the approach to a case in which the action is based on the tort of "invasion upon seclusion." 70 First, the Court of Appeals noted that where an action for wrongful discharge asserts a relationship between the discharge and an invasion of the employee's privacy, the court would examine the facts and circumstances to determine whether "an alleged invasion of privacy is substantial and highly offensive to a reasonable person." 71 Second, as the District Court explained, the Borse court anticipated the use of a balancing test to weigh "the employee's privacy interest against the employer's interest in maintaining a drug-free workplace." 72

The court in Smyth addressed his claim by explaining that Pennsylvania law does not recognize a cause of action for the wrongful discharge of an at-will employee, but that exceptions to the general rule have been made where a mandate of public policy has been violated. 73 The court then listed the recognized exceptions, 74 and stated that the public policy on which the exception is based must be clearly defined. 75 Further, the court outlined the sources of the public policy on which an exception could be based, and pointed to Borse which states that the bases can be found in "legislation, administrative rules, regulation, or decision; and judicial decisions." 76

Without evaluating the sources of Smyth's public policy argument, however, the court evaluated the claim based on the "intrusion of seclusion" framework outlined in the Restatement and adopted by the Court of Appeals in Borse. 77 According to the Borse analysis, a finding that the discharge was "related to" an invasion of privacy which is substantial and highly offensive would merit the conclusion that the discharge violated public policy. 78 First, the court concluded that there is no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management." 79 Second, the court concluded that the reasonable expectation of privacy was lost "once plaintiff communicated the alleged unprivileged messages can be lawfully made." 80 This conclusion by the court implies that the breadth of use of the system is equivalent to access to the communications. Thus, since the whole company uses the system, the whole company has access to the communications, and therefore a person using the system has no expectation of privacy. The court's implication ignores the necessity of a company to use a single network, and further disregards the fact that the messages are not necessarily revealed to the entire system, or even the system administrator. E-mail is not a broadcast to everyone in the company or on the same system. Without a finding of a reasonable expectation of privacy, however, there can be no invasion of privacy.

In determining that Smyth did not have a reasonable expectation of privacy in the messages,
the court placed significant weight on its assertion that the employer did not require the plaintiff to disclose any personal information about himself, and distinguished these facts from the situation in *Borse*, where the employees were subject to urinalysis screening and personal property searches. The court further explained that the "plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system." The distinction drawn by the court, however, fails to account of the employer's conduct in the case. In both *Borse* and *Smyth* the employer is the actor, in some way accessing information about the employee. In a search of personal property, the employer peruses the personal property in search of drugs, or some evidence of misconduct. Incidental to the search would be the disclosure of personal information. The same is true of communications made using an electronic mail system. For whatever reason, perhaps to ascertain the current company morale, the employer browses the e-mail system. Such browsing of the communications contained on the system is certain to reveal personal information about the employee, particularly when the employee has no idea that the messages are intercepted - indeed believes them to be private and confidential. In both cases discovery of the information is predicated upon the employer's action. In *Borse* the employer's action required the participation of the employee and was pursuant to a policy; in *Smyth* the action was surreptitious and directly contrary to the policy. In both cases, then, the employee's privacy is invaded, but in *Smyth* the policy created an expectation of confidentiality which was not honored by the employer.

Finally, the court concluded that even if the employee had a reasonable expectation of privacy in the e-mail messages, Pillsbury's interception of his communications is not a substantial and highly offensive invasion of his privacy. To support this finding, the court again points to its conclusion that the company did not require the plaintiff to disclose any information about himself "or invad[e] the employee's person or personal effects." Almost as an afterthought, the court sought to balance the interests, finding that the company's interest in preventing "inappropriate and unprofessional comments, or even illegal activity over its e-mail system" outweighs the privacy interest the employee may have in the comments or activity.

In ruling for Pillsbury in this case, however, the court simply ignored the company's conduct. In doing so, the court requires no responsibility on the part of the employer, and, therefore, forces the employee to enter a system at his or her own risk, unable to rely on the employer's policy. The decision undermines efforts to establish a satisfactory relationship between employer and employee because the employer is not required to abide by rules of common decency, and it weakens possible protection of employee privacy rights in the workplace.

**B. Bohach v. City of Reno**

In *Bohach v. City of Reno*, the District Court for the District of Nevada addressed the claims of two police officers that the Reno Police Department violated the federal wiretapping statute and their constitutional right to privacy when the Department stored and retrieved messages they had sent over the Department's "Alphapage" message system. The issues were presented to the court terminal, is essentially "e-mail." The court explains the process of sending the message via the Alphapage system as follows. After logging onto any computer in the Reno Department, the user selects Alphapage from a menu, then selects the name of the person with whom the user would like to communicate. Then, the user types the message on the computer, and "sends" the message. The computer screen displays that the message is being processed as it sends the message to the "Inforad Message Directory," and stored in a server file. The computer then dials and via modem, sends the message to a commercial paging company, then disconnects, at which point the computer indicates that the page has been sent, and the commercial paging company completes the message transmission by sending the message to the recipient pager by radio broadcast.
when the officers Bohach and Catalano sought to prevent an internal affairs investigation based on the contents of the messages, and to bar disclosure of the messages. The court found the officers did not have a reasonable expectation of privacy in the messages, and that obtaining the messages from the Alphapage system did not violate the prohibitions in the ECPA.

The court addressed the officers’ Fourth Amendment claim of invasion of a right of privacy by determining whether the officers had an objectively reasonable expectation of privacy in the messages. Several factors led the court to hold that they did not. First, because the system automatically stored communications, “not because anyone is ‘tapping’ the system, but simply because that’s how the system works,” the officers’ expectation of privacy in the messages was reduced. Second, the objectively reasonable expectation of privacy was reduced because the Chief of Police had issued an order when the system was installed notifying the system’s users that the messages would be “logged onto the network,” and that certain types of messages were banned from the system. Further, access to the system was not protected or limited by a special password or clearance. Anyone with general access to the system could “roam at will through Alphapage.” Third, the court pointed to the ordinary course of police station business to record telephone calls made to and from the station. The purpose of the Alphapage system was to provide communication between police personnel and between police and the press, and not necessarily for personal messages. Thus, not only do the limitations and purpose of the system demonstrate a reduced expectation of privacy, even telephone calls from a police station would not enjoy a reasonable expectation of privacy given the ordinary practice of recording.

The court then evaluated the assertion that the retrieval of the messages from the system constituted a violation of the federal wiretapping statute, the ECPA. At the outset, the court noted the inclusion of “electronic communications” in the statute, and explained the statutory distinction between the “interception” of an electronic communication at the time of transmission and “the retrieval of such a communication after it has been put into “electronic storage.” Next, the court determined whether an “interception” occurred, and concluded that it had not. The court asked “how any ‘interception,’ as the word is usually understood, could be thought to have occurred here . . . [since] no computer or phone lines have been tapped, no conversations picked up by hidden microphones, no duplicate pager ‘cloned’ to tap into messages intended for another recipient.” By posing the question the court belied its understanding of the statute. Under the statutory definition, “interception,” or the “acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical or other device,” could occur without the installation of some other device. Therefore, although it stated the statutory definition of an interception, the court resorted to the “usual” or common understanding of the term to determine whether an interception had taken place. The court suggested further that “no one would object” if the computer were merely a “conduit” or a stop along the way to the recipient, if the message were not recorded or stored, since the computer would not have acquired information on the contents or purport of the message. In addition, the court suggested that even if the person did object to the computer as a conduit, it would find implied consent to outside knowledge discrimination policy, and those containing comments on Department policy, were banned from the system.

99 Id. at 1235.
100 Bohach, 932 F. Supp. at 1236.
101 Id. (citing 18 U.S.C. § 2510(12) (1994)).
102 Id. at 1235-36.
103 Id. at 1236.
104 Id.
105 Id. (citing 18 U.S.C. § 2510(4) (1994)).
106 Id.
107 Bohach, 932 F. Supp. at 1236.
of the messages simply because the computer was used to send messages.\textsuperscript{108}

This narrow reading of "interception" fails to recognize the purpose of the statute and fails to account for the capabilities of the technology. By relying on a common understanding of the term "intercept," the court defeats the purpose of enacting legislation which adapts to advancing technology. An intercepting device could be read to be another computer on the system, and it is not necessarily required to be a covert addition to the system. Furthermore, a person reading the message as it passes through the computer conduit, a system administrator, for example, would have "intercepted" the message — for the person has acquired information about the contents of the message. The interception may be inadvertent, but information is acquired nonetheless.

The court continued, however, and found the officers to be objecting not to the fact that the messages passed through the computer, but the messages were stored and subsequently retrieved.\textsuperscript{109} This, the court held, cannot amount to interception because once a message is stored it is no longer a communication, and only "communications" can be intercepted.\textsuperscript{110} Once the court identified the messages as being located in "electronic storage," it needed only to establish the Reno Police Department as the "provider" of the "electronic communications service."\textsuperscript{111} As evidence that the department was the system "provider," the court noted that the software, the pagers and the computer terminals, all necessary to send and to receive messages, are provided by the police department.\textsuperscript{112} Thus, as a "provider" under § 2701(c)(1), the department can "do as they wish when it comes to accessing communications in electronic storage."\textsuperscript{113} The court held, therefore, that the injunction against the police department was properly denied and that the investigation of the officers could proceed.\textsuperscript{114}

III. THE EFFECT OF THESE DECISIONS ON EMPLOYEE PRIVACY IN THE WORKPLACE

These cases demonstrate the unfortunate widening of the gap between employees' right to the privacy of e-mail messages and employer's concern with and right to monitor employees. As the gap widens, however, the employer may not achieve the benefit it seeks. The aforementioned cases demonstrate that an employer is currently able to place liability on the employee for the contents of employee e-mail messages — by discharging the employee for example — and to do so without liability for infringing the employee's privacy. Rather than preventing and reducing its liability, however, by implementing monitoring practices, by asserting more detailed control over employee use of the e-mail, and by failing to abide by its own policies, the employer is making itself susceptible to greater liability for the evils committed using e-mail.

One of the justifications for employer monitoring of employee e-mail is to prevent its use for personal reasons, including acts for which the employer may be liable.\textsuperscript{115} Although the extent of employer liability for employee misconduct committed using e-mail and computer software is not settled, the potential is real and only increased with computer technology. In the context of defamation and slander,\textsuperscript{116} for example, the nature and perception of e-mail contribute to the likelihood that those torts will be committed.\textsuperscript{117} One analysis of employer liability in the context of computer technology notes that torts are facilitated with electronic communications because the messages tend to be more casual and because of the "relatively anonymous nature" of the methods of electronic communication which may "embolden" employees to communicate in such a way they would not otherwise communicate.\textsuperscript{118}

\textsuperscript{108} Id.
\textsuperscript{109} Id.
\textsuperscript{110} Id.
\textsuperscript{111} Id.
\textsuperscript{112} Bohach, 992 F. Supp. at 1236.
\textsuperscript{113} Id.
\textsuperscript{114} Id. at 1237.
\textsuperscript{115} See Interview by Pat Etheridge with Hal Coxson, Management Lawyer and Lewis Maltby, ACLU, in New York, N.Y. (Sept. 1, 1996).
\textsuperscript{116} A claim of defamation is established when: (1) the plaintiff proves the defendant made a false statement of fact; (2) published the statement to a third party; and (3) the statement injured the plaintiff's reputation. Restatement (Second) of Torts § 558 (1977).
\textsuperscript{117} Donald H. Seifman & Craig W. Trepanier, E-mail and Voicemail Systems (Part I), EMPLOYEE REL. L.J. at 5, 18 (Winter 1995-96).
\textsuperscript{118} Id.
tionally, the communications are subject to misinterpreta-
tion by the recipient, are more easily "published," and are frequently stored after the parties have completed the transmission. Therefore, an employee may defame another on the e-mail system, and both the precise language and the fact of "publication" to a third party -- components of the tort -- are preserved for the lawsuit. When defamatory statements are made by an employee within the scope of the employment, the employer may be liable. Not only could the employer be held liable for the defamation committed by the employee, but also defamation committed by the employer would be easier to prove.

Employer liability may be increased by the use of electronic communication in other areas as well. Under the tort of "product disparagement" or trade libel, employers could be held responsible for the message sent by an employee regarding a customer or competitor and his or her goods or business. Employers may also be liable for the conduct of employees who post copyrighted material on the Internet using the company's computers, or where an employee downloads material and distributes it in the workplace. Liability is more likely to attach where the employer is aware that the posting or distribution is occurring. Again, developing a company policy regarding posting information on the Internet has been encouraged as a way of limiting the instances of copyright infringement and providing a potential defense for the employer.

Sexual harassment is another area where liability could be increased as a result of e-mail messages. The ability of employees to send messages anonymously, or to attribute the message to another employee, to retrieve sexually explicit materials from the Internet, and to play "pranks" on fellow employees heightens the possibility that a "hostile work environment" could be created. Importantly, the storage of e-mail messages may assist the plaintiff in establishing the existence of the hostile work environment.

The widespread use of e-mail and the ease with which information can be transmitted poses an additional risk to employers seeking to protect trade secrets. One analysis of the problem notes that since most statutes which protect trade secrets require a showing that the employer made reasonable efforts to keep the information confidential, employers should refrain from transmitting sensitive information using e-mail, and should clarify for employees specifically the information appropriate for communication on the e-mail system.

In recognition of these risks, employers are advised to instruct and to train employees on the proper use of e-mail. Additionally, analysts encourage employers to monitor employee e-mail

---

119 The authors note that whereas verbal communications allow the speaker to "feel out" the audience and to use body language, tone, voice inflection to minimize the impact of the statements, these devices of personal communication are not transferable using electronic mail. Id. Coupled with the tendency not to draft e-mail messages with precision, the inability to communicate voice inflection, for example, the potential for misinterpretation is great. Id.

120 The capability of storing, printing, retransmitting the message to a third party or mistakenly transmitting the message to an unintended recipient are features of e-mail which also heighten the potential for a lawsuit for one of these torts. Id. at 19-20.

121 Seifman & Trepanier, supra note 117, at 20.

122 Id.

123 See, e.g., Hoke v. Paul, 653 P.2d 1155, 1158 (Haw. 1982) (stating an employer is liable for defamatory acts of employee if it is done in the course of employment).


125 "Product Disparagement" or "Disparagement of Quality" is defined as "a false statement harmful to the interests of another." RESTATEMENT (SECOND) OF TORTS § 623A (1977).

126 Seifman & Trepanier, supra note 117, at 22-23.
and strictly to enforce the policies adopted by the companies regarding e-mail. Along with routine monitoring and organizing of the information contained on the employer's computer system, analysts also suggest incorporating a policy which includes the regular deletion of messages and information contained on the company system in order to rid the system of damaging evidence, while avoiding the "negative inference" created by missing data. Thus, the development of company policies tends toward greater control of employee e-mail.

It is a fundamental principle of agency law that when extensive control is exercised by the principal over the agent, it is more likely that the principal will be responsible for the conduct and misconduct of the agent. Indeed, developing company policies on e-mail and encouraging employees to exercise restraint in their use of e-mail may be a means of reducing liability by educating employees and thereby reducing the incidents of the torts or illegal behavior. This control, however, may also increase the liability of the employer. Plaintiffs could claim negligent supervision, or that a "reasonable" employer would have conducted monitoring to find inappropriate use of the system. In addition, a plaintiff could seek to establish a presumption of knowledge on the part of the employer using the existence of the monitoring practice or policy.

By failing to recognize an employee expectation of privacy, the courts in Smyth and Bohach have contributed to the potential extension of liability. The result of these cases is not only that the employee cannot expect privacy in an e-mail message system, and cannot rely on the company policy, but also that the employer will be forced into monitoring every e-mail to prevent misconduct, misuse and abuse of the system. This monitoring reduces what little privacy the employee is currently able to claim. Despite compelling arguments in justification of employee monitoring, when done surreptitiously and in contravention of a stated policy, it will reduce the use of the advancing technology, thus slowing advancement, and, more importantly, restricting the expression and transmission of ideas and speech.

As cases similar to Smyth and Bohach are presented to courts across the country, courts should begin to establish a framework of analysis for the issue. This approach should begin with a recognition of a public policy exception to a wrongful discharge claim where the employee is an at will employee. Although the court declined to break ground regarding a public policy exception in Smyth the opinion provides the starting point. The court states that sources for the public policy "can be found in 'legislation, administrative rules, regulation, or decision; and judicial decisions . . . . Absent legislation, the judiciary must define the cause of action in case by case determinations." The court also cites a case from the Third Circuit which supports the assertion that "a clear mandate of public policy' [is] embodied in a constitutionally or legislatively established prohibition, requirement, or privilege." The treatment given to the public policy claim, however, fails to acknowledge the existence of the ECPA and its protection of electronic communications, including e-mail, as an indication of public policy. The court also overlooks legislation that has been proposed in Congress and state legislatures which has the specific purpose of protecting e-mail. The language in Borse also suggests the possibility of such an exception. Therefore, had the court endeavored to find justification for acknowledging the public policy exception recognizing that termination of employment should not be based on information gained by an invasion of privacy, it could have the basis for the exception in the very sources it cited.

Although it may be harder to justify recognition of a reasonable expectation of privacy in e-mail messages transmitted using a computer owned by the company, via a system operated by the company, especially given the company's technical

137 Id. at 23.
138 David C. Jacobson, Peril of the E-mail Trial, Nat'L L.J. at 1, 22 (Jan. 16, 1995).
139 RESTATEMENT (SECOND) OF AGENCY § 140 (1958).
140 Id. at 23.
141 RESTATEMENT (SECOND) OF TORTS § 317 (1965).
143 Id. (quoting Smith v. Calgon Carbon Corp., 917 F.2d
1388, 1344 (3d Cir. 1990)).
144 Id. at 101; see, e.g., S. REP. No. 541, 99th Cong., 2d Sess., at 14 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568 (indicating a general Congressional intent to protect e-mail.).
145 See, e.g., The Privacy for Consumers and Workers Act, S. 984, 103d Cong. (1993).
ability to retrieve messages and overwrite passwords, the unfairness of a situation which allows the employer to monitor employee communications without restraint is clear. Courts should require adherence by the employer to a company policy by allowing evidence of the existence and implementation of a clear policy of which the employees have notice. Where the company develops policy, notifies employees of its intentions and limits its practice of monitoring capabilities to the guidelines announced in the policy, the company’s liability should be limited, and the employee should be entitled to the measure of privacy provided by the policy.

Allowing employers to limit liability for wrongs committed against third parties using e-mail provided by the employer will encourage employers to develop company policies which employ only limited monitoring; for example, to verify assertions of harassment. It will also encourage employers to adhere more closely to the policies they implement. This will provide the measure of privacy sought by employees, and at the same time will encourage the education of employees on the legality, capability and limits of employer’s monitoring of e-mail messages. This education, in turn, will lead to more responsible and informed use of e-mail by the employees. Instead of being trapped by their own ignorance, they will feel secure in the boundaries and appropriate uses. Both employees and employers will receive favorable results from the open approach to the technology of electronic communications which court imposed requirements of a policy and disclosure will afford.

The benefits to employers of disclosure of the employer’s capabilities were seen in Bohach. The court pointed specifically to explanatory statements given by the Chief of Police when the system was installed. The employees were warned that the messages were “logged onto the system” and were specifically limited in the types of messages which could be sent.

The opinion in Bohach additionally suggests that in employment settings other than a police station employees may be entitled to some expectation of privacy in the messages. The court points to the warnings by the Chief, the fact that anyone could gain access to the system and the messages without a password, the limited number of available recipients (recipients must have an Alphapager), the ordinary and proper course of business of the police station to record phone conversation and the fact that the messages are recorded and stored as a matter of how the system works to establish the “diminished” expectation of privacy in the messages. It may follow in a different situation - where a recipient receives a message at a specific address, where access to the system is protected by a password, where messages or communications from the company are not routinely recorded or stored, but perhaps in fact destroyed or assured by the company to be confidential - that the employee may have a reasonable expectation of privacy.

IV. CONCLUSION

Until the guarantee of privacy is achieved by the development of technology, the courts need to recognize the problem and outline a framework which balances appropriately the privacy interest in the messages with the employer’s legitimate interest in using technology to monitor employee productivity and effectiveness. Employer invasion of employee privacy, however, must be curbed.

148 Id.
149 Id. at 1235.
150 Id.