J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 6(4) 289-303, 1997-98

COMMENT: E-MAIL IN THE WORKPLACE: DEFINING THE BOUNDARIES OF EMPLOYEE PRIVACY

DONNA M. HAWLEY
Law Student, Widener University School of Law

ABSTRACT

Along with other high technology issues, e-mail privacy in the workplace has become a growing concern in recent years. E-mail monitoring has been compared to telephone monitoring and U.S. mail, as well as locker and desk searches. The basic consensus is that as long as employers make it clear they will be monitoring e-mail, the employee will not be able to seek redress. This article explores boundaries of privacy in the workplace regarding e-mail communications and examines recommendations for improvement.

Technological advances have made possible today what was thought to be unthinkable as little as twenty years ago. Compact discs, CD-roms, laptop computers, and laser discs are just a few examples of modern conveniences that were not available until recently. Electronic mail (e-mail) is another form of technology currently experiencing widespread use. E-mail is a faster, more efficient, and cheaper way to communicate than traditional United States mail, interoffice mail, and telephone communications. Consequently, many businesses have implemented e-mail systems for use in their daily operations. In fact, more than twenty million American employees use e-mail to communicate with their coworkers [1].

With so many companies currently using e-mail as a common form of communication, employee privacy concerns arise when employers examine the employee's e-mail messages without the employee's knowledge or permission. Because the technology itself is so new, the law concerning an employee's privacy rights in his/her e-mail communications is unclear at best.

Commentators have based the right of privacy [2] on the idea that one has the "right to be let alone" [3]. Privacy in employment is a rapidly evolving area of

doi: 10.2190/TJQV-Q9J8-3T42-LHCT
http://baywood.com

law [3, § 1.4], and as such, its development needs to be constantly reviewed to keep up with modern technological advances. Sometimes an employer has a legitimate business interest that may infringe on an employee's privacy interests; however, "there are compelling reasons to limit the employer's trespass on employee privacy where no legitimate business reason exists" [3, § 1.4]. Under what circumstances does an employer have a "legitimate business interest" to look at an employee's e-mail communications?

The parameters of this area of the law have not yet been fully tested; however, the few cases that have been litigated, as well as constitutional and statutory law, can provide a basis for setting forth some basic principles and can provide a backdrop for predicting the future of the boundaries of employee privacy rights in e-mail communications. This article explores the employee privacy concerns that are implicated when an employer retrieves, intercepts, or reviews an employee's e-mail communications.

DEFINITIONAL CONSIDERATIONS IN WORKPLACE E-MAIL MONITORING CLAIMS

E-Mail Systems

The way in which an e-mail privacy claim is analyzed may depend on what type of e-mail system is being used. One type of e-mail system is operated by an electronic mail or communications company such as AT&T-Mail, MCI-Mail, or Sprint-Mail [3, § 7.14A (Supp. 1996)]. In this type, a password is issued to each user for access to the system. This password "acts as a security device" and "prevents unauthorized individuals from accessing a user's files" [3, § 7.14A (Supp. 1996)]. The message is typed in by the sender and transmitted through telephone lines owned and operated by the communications company. To access this type of system, a computer, modem, and appropriate software are needed.

The second type of e-mail system is operated by a private entity such as a corporation or a business. This type of system "is completely private." In this system, "[a] private line exists between two points with no connection to a public telephone system" and "the business handles all computer calls within the company and considers these calls its exclusive property" [3, § 7.14A (Supp. 1996)]. Security devices such as "passwords, frequent changes of passwords, encryption of passwords, and multiple-level password entry" can prevent hackers and other employees from gaining access to a user's files, but they do not prevent access by the employer because the employer is the provider of the system [3, § 7.14A (Supp. 1996)].

This distinction is important because the Electronic Communications Privacy Act (ECPA), the most closely related statute thus far, contains certain exceptions that apply to employers if they are providers of the e-mail service. By asserting that the e-mail communications are the property of the company and that the

property needs to be protected, the employer can protect its rights by accessing and divulging the information from the e-mail communications [4].

Intercepted Communications v. Stored Communications

Another important distinction to make is whether the e-mail message was retrieved from storage or intercepted while in transmission. The ECPA defines "interception" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" [5]. The ECPA defines "electronic storage" 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 the backup protection of such communication" [6]. This distinction is meaningful because "the degree of privacy protection afforded wire and electronic communications appears to differ based on whether the communication is being transmitted, and thus protected under § 2511 of the ECPA, or in electronic storage, which subjects the communication to § 2701 protection" [7]. The distinction may or may not be important depending on what source of law a plaintiff-employee uses and what type of claim is brought.

REDRESSING GRIEVANCES

To redress an infringement on an employee's privacy rights, several sources of law should be examined. Among those are constitutional law, statutes, state law, and common law. Some sources may be more helpful than others in specific situations. The law is ambiguous regarding employer intrusions on e-mail; therefore, each individual case must be closely scrutinized in the context of each different source of law.

Constitutional Law

The Fourth Amendment to the United States Constitution is implicated only when there is a public employer involved. This is because a public employer is acting for the state [8]. The Fourth Amendment protects against unreasonable searches and seizures; in this context, an employee of a government entity "must show that he has a reasonable expectation of privacy" [4, p. 554]. *United States v. Katz* [9] established a two-pronged test for cases involving an allegation of a violation of Fourth Amendment rights. First, the employee must show that s/he had a subjective expectation of privacy. Second, the employee must show that the expectation of privacy was reasonable.

Because a password is issued to the sender and because the sender is transmitting the message to a specific recipient who can access that message only with his/her own password, it is clear an employee has a subjective expectation of

privacy [4, p. 555]. In determining whether that expectation of privacy is reasonable, courts will generally take into consideration such factors as the employee's property interest or rights, the surrounding circumstances of the search of the property interest, and general office practices [4, p. 558].

If e-mail is looked at as a form of personal mail, an invasion of privacy occurs when an employer invades an employee's e-mail. Because personal mail is always addressed to a specific recipient, an individual has a "reasonable expectation of privacy in their [sic] personal mail" [4, p. 558]. Even if the employer owns the property or provides the service, the only way to avoid the employee's expectation of privacy is to inform all employees that their e-mail will be monitored. It is important, however, to keep in mind that Fourth Amendment protections apply only to government employees.

Statutory Law

The Electronic Communications Privacy Act

In the area of e-mail communications, the Electronic Communications Privacy Act of 1986 is the most significant statute thus far. The ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 [10], and is commonly known as the federal wiretapping statute. This statute prohibits the interception of electronic communications, but contains certain exceptions that could be interpreted to exclude privacy protections for employees [11].

The three exceptions of the ECPA that may limit employee e-mail privacy protections are noninterstate systems, prior consent, and business use [11]. First, an e-mail system within a company "may not be covered by the ECPA" because "the definition of 'electronic communications' under the statute only pertains to communication that 'affects interstate or foreign commerce' " [12]. It has been suggested that the only way an intracompany e-mail system may be covered is if it "crosses state lines or . . . connects to an interstate network"; however, judicial interpretation is needed to determine whether this is in fact the case [11, p. 153].

Second, if one of the parties has given prior consent, the interception of e-mail is allowed. Consent may be express or implied. If consent is not expressly given, courts may analyze different aspects of the employer-employee relationship to determine whether implied consent was given based on the surrounding circumstances. If a company has a specific written policy on e-mail monitoring, implied consent would be given by the employee as long as the monitoring did not exceed the terms of the company policy. Even if the company policy stated that monitoring *may* be done (but will not necessarily be done), the employee has not given implied consent to be monitored. "[T]he legality of *E-mail* monitoring under the prior consent exception may depend on the specificity and clarity of the company's monitoring policy" [11, p. 154].

Third, the business use exception allows employers to intercept e-mail communications in the "ordinary course of business." Of the two provisions of the

ECPA addressing business use exceptions, only one seems to be helpful in analyzing an e-mail monitoring claim [13]. Under this exception, electronic communication service providers or their agents may intercept a communication in the ordinary course of business [14]. Providers of electronic communication service would include public e-mail networks, as well as employers who provide their own e-mail networks. The interception must be done in the ordinary course of business and "employers would need to prove that the monitoring was necessary to render service or to protect their rights or property" [11, p. 156]. In most cases, this excludes employers from monitoring personal calls, except to the extent necessary to establish that it is in fact a personal call. "[I]f the courts analogize E-mail interceptions to telephone extension monitoring, employers may be able to prove a legitimate business reason for the monitoring, provided that the monitoring does not include reading personal E-mail in its entirety" [11, p. 157].

Stored electronic communications are governed by Title II of the ECPA [15]. Employers who have implemented a private e-mail system are most likely exempted from the access and disclosure prohibitions because they are the providers of the system [16]. An employer who subscribes to an e-mail service would probably not be able to utilize this exception. In the case of stored electronic communications, it has been urged that "Congress . . . act based on the assumption that E-mail be provided the same protection afforded to first class mail" [17]. Employee expectations of privacy may be created if the employer treats e-mail communications similar to first class mail and does not have a specific policy that restricts e-mail use to business purposes [3, § 7.14A (Supp. 1996)].

The ECPA provides some protections for employee privacy in e-mail communications, but employers are given wide latitude to monitor employees under this statute. The exceptions seem to permit monitoring of e-mail within a privately operated system, and there is even the possibility that e-mail interceptions will be allowed when the provider is a public communications company because the employer is acting as its "agent." It is urged that employers should "look to employee expectations of privacy deemed reasonable in other contexts [such as first class mail]" [17, p. 929].

Thus, in analyzing an e-mail monitoring case, a distinction should be made as to whether the e-mail was intercepted or retrieved from storage. Although this distinction may be more difficult to make than in telephone or voice mail communications, the differing standards of the ECPA make it an important distinction. E-mail interceptions can be compared to telephone interceptions, whereas stored e-mail can be compared to first class mail. Under the ECPA, employers are more likely to be allowed to look at their employees' e-mail communications (as long as they are the system provider) if the e-mail is deemed to be in storage than if the e-mail is deemed to be intercepted. According to one commentator, the ECPA's provisions, when applied in e-mail communications, are irrational

because "the limitations imposed on employer interceptions of wire or electronic communications vanish once the same communication is in storage" [7, pp. 248-249]. In the context of intercepted e-mail, the "business use" exception seems to be the most damaging to employee privacy rights; however, the issues present here have not yet been litigated enough to entirely rule out employee privacy violations.

The National Labor Relations Act (NLRA)

The National Labor Relations Act (NLRA) can provide some guidance in situations where a company has employees who do not come into an office, but rather, work at home and communicate through their computers and e-mail [18]. The purpose of the NLRA is "to protect meaningful communication among employees for the purposes of mutual aid and protection" [18]. The NLRA may be violated if an employer places a complete ban on all nonwork-related use of e-mail because it would prevent employees from acting collectively, which would be a violation under the NLRA. One case ruling stated "[i]t is not . . . within the province of an employer to promulgate and enforce a rule prohibiting union solicitation by an employee outside of working hours, although on company property" [19].

To ensure that the NLRA is not violated, employers need to be cautious when placing bans on nonwork-related e-mail use if they have employees who work outside of the office and away from other employees. Although a complete ban may protect an employer by taking away an employee's expectation of privacy, it may infringe on the employee's right to collectively bargain [20]. It is possible the NLRA may be implicated even when only one employee works outside the office and communicates only through e-mail because that employee may be excluded from communication with other employees. Only time and judicial interpretation will tell.

State Statutes

Several states have statutes that are more restrictive than the ECPA and require that all parties involved give their consent to be monitored, rather than just one party [11, pp. 158-159]. The requirement that all parties give their consent would only be implicated when the person with whom the employee is communicating is a nonemployee rather than an employee of the same company. States are able to enact stricter laws to provide more privacy protections than federal law, and "unless a conflict between the law exists, the state law will prevail" [11, p. 158]. At the present time, however, state law leaves private sector employees virtually unprotected from employer e-mail monitoring [21].

A case in point is *Shoars v. Epson America, Inc.* [22]. Shoars was an employee in the Information Resources Department of Epson America, Inc. One of her main responsibilities was to support other employees in their use of e-mail. She was directed by her supervisors to inform all employees that their e-mail

communications would be confidential. She did not know that her supervisor had placed a tap on the e-mail system that downloaded and printed all sent and received e-mail messages. When she confronted her supervisor, she was told to keep quiet about her discovery. She was fired shortly thereafter when she requested a password that her supervisor could not access.

Shoars filed suit under California Penal Code section 631, which requires that *all* parties consent before a communication may be tapped [23]. The Superior Court of California held that section 631 did not cover e-mail. The court contended that in order for there to be an invasion of privacy through wiretapping, a plaintiff must have had an expectation of privacy. Here, the court did not find that Shoars had an expectation of privacy, and hence sustained Epson's demurrer, finding that Shoars had failed to state a claim.

Commentators have asserted that the court employed flawed reasoning to come to the conclusion that e-mail is not covered under the state wiretapping statute [24]. Furthermore, it has been urged that "[s]tate courts should not exclude E-mail from the purview of their state statutes [which are analogous to the ECPA] simply because those statutes neglect to mention the words 'electronic mail' " [24, p. 231]. The California state court, just like the many other sources of law, favored the employer's rights over the employee's privacy rights. Regardless of how the court *should* have decided, the way that it *did* decide makes it apparent state statutes do not adequately protect the privacy interests of employees [25].

Common Law Causes of Action

Depending on the facts in a particular case, "privacy expectations [of an employee] could subject the employer to liability for invasion of privacy, defamation, intentional infliction of emotional distress, fraudulent misrepresentation, or intentional interference with contractual relations" [3, § 714A (Supp. 1996)]. Some commentators have noted that the most applicable common law cause of action to e-mail interception or accession is the tort of intrusion upon the seclusion of another [11, p. 161; 26, pp. 345, 374]. This tort states that "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his or her private affairs or concerns, is subject to liability to the other for invasion of his or her privacy, if the intrusion would be highly offensive to a reasonable person" [27]. It has been argued that this tort protects an employee from "electronic eavesdropping" and from "unreasonable intrusions by employer searches" [11, p. 161; 26].

Although courts do not have a set list of criteria, there are four factors that courts take into consideration when deciding a case involving the tort of intrusion. Those factors are: "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 a reasonable person'; and 4) whether the infringer had a legitimate purpose warranting the intrusion" [11, pp. 162-163]. It has been

suggested that e-mail passwords be compared to padlocks on lockers [11, p. 164]. However, specific facts need to be taken into consideration, such as whether the e-mail system is publicly operated by a common carrier or privately operated by the company and whether the password is created by the employee or assigned by the employer [26, pp. 376-377]. These facts will help determine whether the employee had a reasonable expectation of privacy in his/her e-mail communications.

If the employer has a legitimate business interest, the employee's privacy interests can be overridden. Thus, if there is a legitimate business interest in searching and monitoring an employee's e-mail, the employer will not be held liable. To summarize, "[t]he critical issues in determining tort liability for E-mail interception are thus whether employees have a reasonable expectation of privacy in their E-mail correspondence and whether their employer offers legitimate business justifications for the intrusion" [26, p. 378]. Commentators agree that the employer should publish and post an e-mail monitoring policy that puts employees on notice that e-mail messages may be monitored; the policy should be clear enough to warn employees so they will not have a false sense of privacy [7, p. 250; 17, p. 947; 26, p. 388].

INADEQUACIES OF CURRENT LAW

Many commentators agree that the current state of the law is inadequate to properly protect employee privacy interests. The law at this point clearly favors employers. Commentators warn, however, that "[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances" [28]. The Fourth Amendment does not protect private employees; the ECPA contains exceptions allowing employers to monitor e-mail; most states have not enacted adequate protections; and the common law invasion of privacy tort is simply not adequate to keep up with growing technology.

Previously Proposed Legislation

It has been suggested that new legislation is needed that deals specifically with electronic monitoring [26, p. 408]. In 1993, the Privacy for Consumers and Workers Act (PCWA) was proposed to Congress [29]. By the end of the 104th Congress, neither the House nor the Senate had passed the bill. This is probably just as well because the PCWA did not "represent a promising avenue for E-mail protections" [26, p. 409]. The deficiencies of the bill lie in the fact that e-mail is excluded from its definition of electronic monitoring and differing levels of monitoring are allowed based on the employee's length of employment. The standards "work to increase employee privacy, [but] they place unnecessarily unbending obligations on employers that frustrate the ability of employers to engage in monitoring in a manner best suited to the employer's particular business context" [26, p. 409].

The most important deficiency, however, is that both the House and Senate version of the PCWA actually "validates the employer's ability to conduct intrusive monitoring practices and further insulates employers from liability under the law" [26, p. 410]. Basically, under the proposed statute, employers must notify employees that they will be monitored; however, the scope of the monitoring is not effectively limited, thus allowing employers to look at the content of all work-related e-mail communications. "[S]imply notifying employees of potential monitoring does not alleviate the privacy burden of intrusive employer practices because most employees do not bargain for their employment and must either accept their employment conditions or risk termination" [26, p. 410]. Thus, previously proposed legislation should not be a model for future legislation because it does not adequately protect the privacy rights of employees.

New Legislation Needed

Even though courts can take a judicial activism stance by extending and restructuring the common law right of privacy to include employee e-mail protections, this is not a plausible response to the need of workplace e-mail privacy because common law precedent would basically have to be abandoned. Similarly, enacting state laws is not adequate because uniform levels of protection are needed. The only sound solution is federal legislation that strengthens employee privacy rights [26, pp. 410-411].

One commentator's proposal for a new federal monitoring law suggests that the policy adopted "must be flexible and aimed at preventing unreasonable intrusions relative to varying types of business operations, organizational needs, and employee privacy needs" [11, p. 172]. This proposal also suggests that the policy should be broad enough to cover similar surveillance and any future technological advances. The federal policy should require that employers "1) have a 'legitimate business purpose' for engaging in monitoring; 2) use the least intrusive means possible to achieve the business objective; 3) limit the access, use, and disclosure to information reasonably meeting that objective; and 4) provide reasonable notification of the monitoring and its use" [11, p. 172].

This commentator also suggested it should be imperative for employers to develop a company monitoring policy that falls within federal guidelines of reasonableness and a company should be required to achieve certain objectives [30]. The author stated "[t]he restrictiveness of a company's E-mail policy will depend on the specific work environment and the needs of both the company and the employees" [11, p. 173].

Another commentator suggested a "compelling business interest" standard should be established in any new federal statute governing e-mail communications in the workplace [26, p. 416]. The employer would have to satisfy this standard to justify an intrusion into the content of an employee's e-mail. The standard would apply to both company-owned and public e-mail systems.

Transactional information would still be allowed to be monitored, subject to the traditional tort standard that balances an employee's reasonable privacy interests against an employer's legitimate business interests. It would make no difference whether the employee was given notice that e-mail would be monitored [26, p. 416].

The author of this proposal expressly rejected the notion of mandating an employer notification policy because "any legislation relying on employee notice to safeguard employee privacy is sorely deficient because notification alone ultimately serves to institutionalize a marginal view of privacy and legitimize practices that infringe upon human dignity" [26, p. 417]. Basically, by not relying on employer notice in statutory language, the employer would be prohibited from taking away all employee expectations of privacy; thus, it would not be left in the employer's hands to determine how much privacy its employees are entitled to.

Opponents of the "compelling business interest" standard may argue that "employers will simply dismantle and cease operating their internal E-mail networks" because if they cannot monitor their employees' e-mail, they will be left at a disadvantage [26, p. 423]. Realistically, if employers want to keep up with the business world, they will have to keep up with growing technology. The use of e-mail has many economic benefits, and employers will not overlook this simply because they are not able to intrusively monitor their employees. If an employer discontinues the use of e-mail, "the ability to recapture any initial operating costs expended in establishing the network and training employees in how to use the system" will be destroyed [26, p. 423].

As discussed below, limiting e-mail monitoring does not decrease efficiency and productivity, but actually increases it, which leads to increased economic benefits. Employers who do not currently have e-mail systems will "install such networks even if they sense that an inability to monitor the content of communications may result in a marginal decrease in efficiency or productivity" because the significant benefits of using an e-mail system will outweigh any such marginal decreases [26, pp. 423-424]. The author of the proposal summed it up by stating "enacting the compelling business interest standard [in a federal statute] will protect important privacy interests, maintain workplace benefits arising from E-mail communications, and even increase employee efficiency and productivity in many contexts" [26, p. 424].

Of the proposals mentioned here, the second is the better of the two. It takes into consideration the fact that simply "giving notice" does not justify taking away an employee's privacy rights. Additionally, it makes no distinction between public and private e-mail systems or between intercepted e-mail and stored e-mail. Moreover, applying this standard would still "allow monitoring in extreme circumstances" and would thus allow employers to access an employee's e-mail communications if necessary [26, p. 418]. A federal statute that follows this proposal will adequately protect the privacy rights of employees.

EMPLOYERS SHOULD VOLUNTARILY LIMIT E-MAIL MONITORING

Setting aside legal issues for a moment, employers should consider implementing a policy that limits or completely abolishes e-mail monitoring. Although there are some benefits of monitoring employee e-mail, there is evidence to suggest increased efficiency does not come from increased monitoring. It comes from developing a good morale among employees by ensuring their dignity and respect.

Benefits of E-Mail Monitoring

The benefits of e-mail monitoring are few and are often overridden by the benefits of allowing employee privacy in e-mail communications. Some employers argue that electronic monitoring is necessary "in order to investigate and prevent theft, fraud, insider trading, drug dealing, and other illegal conduct, as well as to ensure productivity, efficiency, and quality control" [11, p. 145]. Some of those professed benefits, such as productivity, efficiency, and quality control are certainly debatable. An employer may also benefit from electronic monitoring by being able to evaluate employees and ensure that customers are being treated properly.

Moreover, employers benefit because they may be able to use the information they acquire from electronic monitoring to "protec[t] themselves from liability for acts of their employees" [31, p. 138]. Under the doctrine of *respondeat superior*, an employer is held liable for the tortious acts of employees "if the act was committed within the scope of the employee's employment" [31, p. 140]. Proponents of e-mail monitoring may argue that "[w]ithout the ability to monitor the employee, an employer would lose the control from which the liability theoretically arises" [31, p. 140]. Although this may be true in telephone monitoring situations where the employers need "to protect themselves from product liability suits resulting from information given out by their operators" [31, p. 140], this is not the case for e-mail monitoring. E-mail headings can be monitored without being completely intrusive into the content of the message to ensure that no illegal activity is going on. In addition, e-mail communications among employees are not generally distributed to mass markets as is the case with telemarketing or "800" information lines.

Another purported benefit to employers is information security. Sensitive data and trade secrets need to be protected by employers. Also, an employer may argue that monitoring is necessary to prevent fraud or sabotage, or even drug dealing by employees. Intrusive e-mail monitoring is not the answer. Again, e-mail headings can be monitored for transactional information to determine whether an employee is sending or receiving numerous messages to a suspicious e-mail address.

Benefits of Limiting E-Mail Monitoring

Electronic monitoring actually decreases work quality, as well as worker efficiency and productivity, because it increases stress levels among employees. Benefits of limiting monitoring include increased productivity, better service quality, fewer employee grievances, less employee absenteeism, and better morale among employees. These benefits "presumably derive both from the dignity and respect employees feel from the knowledge that they are not constantly being monitored and from the fact that employees worry less about identifying a sharp line between their work and personal lives" [26, p. 419].

Studies have been conducted that indicate employees who are monitored experience more stress and stress-related illnesses than employees who are not monitored [26, pp. 420-421; 31, pp. 141-142]. This leads to diminished productivity and unhealthy employees. In fact, recent research indicated "monitored employees reported more wrist, arm, shoulder, neck, and back problems than those not monitored" [31, p. 141]. Employers should be aware that if they decide to intrusively invade an employee's privacy by electronic monitoring, health insurance costs will probably dramatically increase. One commentator stated that "[i]t is ironic that the monitoring, which was intended to increase productivity, actually causes the employee increased stress resulting in diminished productivity. The monitoring, therefore, can actually be counterproductive" [31, p. 142].

An example of how refraining from monitoring employees dramatically increased productivity is the stance that Federal Express took. They reported their employees worked much more productively when they started to monitor departments as a whole, rather than individual employees [31, p. 142]. Similarly, West Virginia's telephone company achieved high quality service and experienced no decline in productivity when it ceased secret surveillance of its employees. Although these studies generally refer to telephone and other electronic monitoring, the same principles hold true for e-mail monitoring. Any invasion of an employee's privacy that indicates a complete lack of trust by the employer can produce these stress-related complications. An additional concern for employers is that "th[e] perception of mistrust and unfairness resulting from employer monitoring practices may motivate employees to seek union representation" [26, p. 421].

Another benefit employers gain by voluntarily limiting employee e-mail monitoring is that it encourages employees to use the e-mail service. E-mail is cheaper to use and the message is conveyed faster than other forms of communication such as telephone, fax, or mail. In pure economic terms, it is in the employer's best interest to promote the use of e-mail once they have a system in place.

If employees know or even think they are being monitored, they will be more likely to communicate by other means that have more privacy protections. They may also be more hesitant in what they write in an e-mail communication, which

could lead to "miscommunication and ill-informed workplace decision making" [26, p. 422]. For an e-mail system to be used effectively, some degree of confidentiality is needed.

Many corporations have already begun to voluntarily limit employee monitoring because of the demonstrated benefits. For example, IBM, one of the country's largest corporations, "believes its privacy policies make smart business sense because its actions have boosted employer-employee relations" [26, p. 422]. Other companies that have implemented employee privacy policies include Equitable Life Insurance, Citibank, and Bank of America. Additionally, US West and Northern Telecom "have voluntarily decided to make electronic monitoring less intrusive after recognizing the health risks and job stress that result from such monitoring" [26, pp. 422-423].

The many benefits of limiting e-mail monitoring outweigh the benefits of intrusive e-mail monitoring. Economic benefits, increased employee morale, and increased efficiency indicate invasive monitoring of employees is harmful to employers. Until the law in this area is more fully developed, employers should consider voluntarily restricting or prohibiting e-mail monitoring.

CONCLUSION

At the present time, the law does not adequately address privacy concerns of employees in their e-mail communications. Constitutional law, federal and state statutory law, and common law do not provide an adequate avenue of relief for employees whose e-mail is or has been monitored. If left to current standards of law, the right of privacy will erode or disappear in the face of technological advances. Allowing an employer to invasively monitor an employee's e-mail communications is just one step in the deterioration of privacy.

Previously proposed legislation should not be a model for future proposals because it is inadequate to address employee privacy concerns. The "compelling business interest" standard should be used in any future legislation because it rejects the notion that giving notice to employees that they will be monitored excuses the employer from any infringements on an employee's privacy. Currently, in order to escape liability, the employer should publish and post a policy explaining to what extent employee e-mail communications will be monitored [32]. However, the employer should not be able to summarily decide how much privacy their employees are entitled to by simply "giving notice." Since most employees are in a position where they need a job because they need the money, "giving notice" can be seen as a way for employers to basically buy their employees' privacy rights. Putting a price on privacy rights is contrary to the very essence of our existence. Privacy should not be up for sale to the highest bidder.

Until the law catches up with technology, the best thing for an employer to do is to voluntarily limit its e-mail monitoring policy. Less monitoring means higher efficiency, more productivity, higher employee morale, and better

employer-employee relations. By ensuring that employees maintain their dignity and respect, employers gain the benefits of employees who take pride in their work. E-mail monitoring may be done to a certain extent to protect the interests of the company, but should not be completely invasive or without a legitimate business purpose.

* * *

Donna Hawley is a third year student at Widener University School of Law.

ENDNOTES

1. Jill L. Rosenberg, *Legal Issues Surrounding Employee Hiring, Privacy and Investigations*, 547 Practicing Law Institute Litigation and Administrative Practice 569, 616 (1996).
2. The right of privacy was originally stated as the "right to privacy" by Samuel D. Warren and Louis D. Brandeis in their 1890 article entitled "The Right to Privacy." The concept of privacy is generally said to have originated from this article.
3. K. H. Decker, *Employee Privacy Law and Practice* § 1.3 (1987).
4. Lois R. Witt, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 Dickinson Law Review, pp. 545, 553 (1992).
5. 18 U.S.C. § 2510(4) (1988).
6. 18 U.S.C. § 2510(17)(A)-(B) (1988).
7. Thomas R. Greenberg, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U.L. REV. pp. 219, 234 n. 80 (1994).
8. *O'Connor v. Ortega*, 480 U.S. 709, 714-15 (1987).
9. *United States v. Katz*, 389 U.S. 347 (1967).
10. 18 U.S.C. §§ 2510-2520 (1970 & Supp. 1994).
11. 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. pp. 139, 151 (1994).
12. [11, at 152 (quoting 18 U.S.C. § 2510(12) (Supp. 1994)].
13. The other provision is relied on in cases where a telephone extension is used to monitor calls. This exception requires that telephone or telegraph equipment be used in the ordinary course of business. This is not a major concern in e-mail monitoring cases because a court would be hard pressed to find that a software program, computer, or a network manager's modem is telephone or telegraph equipment [11, p. 156].
14. 18 U.S.C. § 2511(23)(a)(i) (Supp. 1994).
15. 18 U.S.C. §§ 2701-11 (1988).
16. *See* 18 U.S.C. §§ 2701-02 (1988).
17. Julia Turner Baumhart, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 LABOR LAW, pp. 923, 928 (1992) (citing Office of Technology Assessment (OTA), Federal Government Information Technology: Electronic Surveillance and Civil Liberties, pp. 45, 51-52 (1985)).
18. *See* Elena N. Broder, *(Net)worker's Rights: The NLRA and Employee Electronic Communications*, 105 YALE L. J. p. 1639 (1996) (arguing that nontraditional,

geographically separated employees have the right to communicate over an e-mail system about nonwork-related topics).

19. *Republic Aviation Corp. v. NLRB*, 324 U.S. 793, 803 n.10 (1945) (quoting Peyton Packing Co., 449 N.L.R.B. 828, 843 (1943)).
20. For a complete discussion of how the NLRA protects an employee's right to bargain collectively through e-mail when the employee does not work in the office with other employees, see [18].
21. For a discussion of more restrictive statutes that have been proposed but never made into law, see [11, pp. 158-161].
22. *Shoars v. Epson America, Inc.*, No. B073243 (Cal. Ct. App.), *Review denied*, No. S040065, 1994 Cal. LEXIS 3670 (Cal. June 29, 1994). *See also Flanagan v. Epson America, Inc.*, No. BC007036 (Cal. Super Ct. Jan 4, 1991) (companion suit to *Shoars* where Epson employees brought a class action suit against Epson under section 631 of the California Penal Code).
23. CAL. PENAL CODE § 631 (Deering 1983 & Supp. 1992).
24. *See* Steven Winters, Comment, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. pp. 197, 228-231 (1993).
25. For a detailed description of *Shoars*, see ELLEN ALDERMAN & CAROLINE KENNEDY, *The Right to Privacy*, pp. 310-17 (1995). Alfred A. Knopf, Inc., 1995.
26. Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. p. 374 (1995).
27. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
28. [7, p. 251 (quoting HOUSE COMM. ON THE JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, H.R. REP. NO. 647, 99th Cong., 2d Sess. 19)].
29. H.R. 1900, 103d. Cong., 1st Sess. (1993); S. 984, 103d Cong., 1st Sess. (1993).
30. For a discussion of the objectives the author listed, see [11, p. 173].
31. Shefali N. Baxi & Alisa A. Nickel, *Big Brother or Better Business: Striking a Balance in the Workplace*, 1994 KAN. J.L. & PUB. POL'Y 137, pp. 138-140 (1994).
32. For a sample corporate e-mail policy, see MATTHEW W. FINKEN, *Privacy in Employment Law*, p. 434 (1995). BNA Books, 1995.

Direct reprint requests to:

Donna M. Hawley
60 Edwards Road
Brick, NJ 08723