Electronic Communication in the Workplace—Something's Got to Give

Kenneth A. Kovach, Sandra J. Conner, Tamar Livneh, Kevin M. Scallan, and Roy L. Schwartz

Every day, millions of American workers use their e-mail and Internet systems, confident that their day's transactions are private. But nothing could be further from the truth. According to a major 1997 survey by the American Management Association, 63 percent of large and mid-sized companies acknowledged that they oversee employees through one or more electronic surveillance systems. Almost a quarter of those companies do not let their employees know they are being monitored.

The impact of e-mail has revolutionized the workplace. A poll reported by Kopp (1998) estimates that 90 percent of large companies, 64 percent of mid-sized companies, and 42 percent of small firms currently use e-mail systems. The same poll found that more than 40 million employees correspond via e-mail, and the number is expected to increase by about 20 percent each year. These statistics are indicative of the popularity of electronic communication in today's workplace. E-mail technology has facilitated more efficient interoffice communications, as well as external communications with clients, customers, and other businesses. It has also expedited personal transactions; in many instances, e-mail has effectively replaced the hand- or typewritten note and letter of memorandum.

The unique nature of e-mail as a communication media warrants special consideration regarding privacy. Although it may be used as a substitute for making a telephone call, there is a big difference between the two. The telephone call is transitory—ending when the phone is hung up—whereas an e-mail note is permanent. Moreover, e-mail can much more easily be examined by a third party without the knowledge of the communicating parties.

Employee privacy is colliding with employer rights in the ongoing battle over e-mail at the office. Who will—and should—win?

As technology becomes faster and cheaper, concerns about workplace privacy issues continue to mount. The impressive advancements in computer communications have created many new problems, and in some cases increased the severity of old ones. It is surprising that despite this growing threat to privacy, there is no legal remedy for employees should their privacy be invaded by their employer. Federal and state courts, for the most part, have upheld employer monitoring, according little or no weight to employee privacy interests—possibly because they do not understand the intrusiveness of the new monitoring technology in the workplace. Neither Congress nor state legislatures have acted to fill the void or provide comprehensive statutory protection for workers. Privacy, ostensibly one of society's most cherished values, is gradually disappearing from the workplace. According to Fader (1998), "American laws don't protect worker privacy very well. We differ from Europe and most industrialized nations. They stringently limit the employee data companies collect, store, and disseminate. We have no such laws."

LEGAL IMPLICATIONS

The right to privacy in the employment context usually derives from the Fourth Amendment to the U.S. Constitution, which reads:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Because the Constitution applies to actions of the state, public sector workers have the provision of appealing directly to the "reasonable expectation of privacy" standard established by the Supreme Court ruling in *Katz v. United States* (Rodriguez 1998). Private sector employees do not enjoy the same level of privacy protection because actions of private employers rarely constitute "state action," which would open the avenue of appeal directly to the Constitution. Because constitutional rights primarily protect citizens from the government, state action is required before a citizen can invoke such a right. The manner in which a government employer treats its employees is by definition a state action. The manner in which a private employer treats its employees is not. Because of this dichotomy, public sector employees enjoy far greater privacy rights than those working for private firms.

"In some cases, private sector employees have not been protected against even the most outrageous forms of employer intrusion."

For the typical private sector employee, then, the only sources of legal protection against intrusive employer surveillance are claims brought under various state statutes or the common law tort "invasion of privacy." The protection provided by these remedies varies widely from jurisdiction to jurisdiction. In some cases, private sector employees have not been protected against even the most outrageous forms of employer intrusion.

To examine the legal implications of e-mail monitoring in the workplace, it is first necessary to consider the circumstances that motivate employers to monitor their workers. One is the ease with which an employer may conduct monitoring. Yet another is the perceived need to curb misuses or abuses of an e-mail system provided and maintained by the employer. Misuse might take the form of wasted time spent sending personal messages to friends, family, or coworkers during business hours. More serious abuses could involve sending harassing messages to coworkers or revealing trade secrets to rival companies.

In the absence of constitutional protection, employees are increasingly looking to Congress and their state legislatures for statutory protection. In response to Congress's perception that abuses associated with new technologies pose a substantial risk to civil liberties, the Electronic Communications Privacy Act (ECPA) of 1986 was enacted. The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which merely proscribed the unauthorized interception of wire and oral communications. Essentially, it extended Title III's existing prohibitions against the unauthorized *interception* of electronic communications.

Thus, explains Kopp, Title III and the ECPA together prohibit intentional or willful interception, accession, disclosure, or use of one's oral or electronic communications. The protections extend to cover the intentional interception of communications by unauthorized individuals and third parties, as well as government agents.

However, the ECPA *does not explicitly* offer protection from employers who access or intercept the electronic communications of *their own* employees. Instead, it appears to offer protection only from the unauthorized interception from *outside parties,* or from another employee who has exceeded his authority when accessing, intercepting, or disclosing information on a private corporate system.

Although none of the provisions in the ECPA appear to limit its applicability to employer monitoring of employee e-mail, Kopp discusses three primary exceptions it does contain that may have the same practical effect: the provider exception, the ordinary course of business exception, and the consent exception.

Provider Exception. The provider exception contained in the ECPA generally exempts e-mail service providers from the ECPA prohibitions against interception or accession of e-mail communications in the workplace. A private employer will be exempt from ECPA liability *so long as it is the direct provider of the e-mail system.* This effectively reserves to employers the unrestricted right to monitor employee e-mail. However, the exception may not apply to employers that merely provide e-mail service through a common carrier such as AOL.

Ordinary Course of Business Exception. The ordinary course of business exception to the ECPA, also known as the business extension exception, states in essence that information transmitted in the ordinary course of business is excluded from the definition of "information transmitted by electronic, mechanical, or other devices," as defined in the ECPA. This exception has yet to be applied to e-mail communications in the workplace.

The Consent Exception. The consent exception to the ECPA generally applies in the event that one party to the communication has

given prior consent to the interception or accession of the communication. Thus, as long as the communication is intercepted by a person who is either a party to it or has expressly consented to such interception, the prohibitions contained within the ECPA will not apply.

Common Law Torts

Because of the lack of clear constitutional or statutory protection, the primary source of employee privacy protection in the private sector workplace has been state tort law. According to Kopp, tort law recognizes four distinct torts protecting the right of privacy:

1. unreasonable intrusion upon the seclusion of another;
2. appropriation of another's name or likeness;
3. unreasonable publicity given to another's private life; or
4. publicity that unreasonably places another in a false light before the public.

The tort most closely associated with e-mail monitoring in the workplace is the "intrusion upon seclusion" tort. It holds that one who intentionally intrudes, physically or otherwise, on the solitude or seclusion of another, or another's private affairs or concerns, is subject to liability for invasion of privacy if the intrusion would be highly offensive to a reasonable person. In holding that the invasion may be "physical or otherwise," this tort could possibly be extended to protect against e-mail monitoring. It also imposes a standard of objective reasonableness. Thus, in deciding whether the intrusion is into a private matter, courts require not only that the employee have a subjective expectation of privacy, but also that the expectation be objectively reasonable.

The common law tort of invasion of privacy has been applied in two recent cases involving e-mail monitoring in the workplace, both discussed by Kopp. In *Bourke v. Nissan Motor Corp.* (1993), the plaintiffs brought action against their employer for intercepting and reviewing several personal e-mail messages. In rejecting their claim of tortious invasion of privacy, the court held that the employees did not have a reasonable expectation of privacy in their e-mail communications because they had signed a waiver stating that e-mail use was limited to company business. The court also noted that the employees were aware that other coworkers had read their e-mail messages in the past, even though they were not the intended recipients of the messages. Further, the court rejected the plaintiffs' argument that a subjective expectation of privacy existed by virtue of having personal passwords to access the e-mail system, as well as their being told to safeguard their passwords.

The most recent case to address the common law tort of invasion of privacy is *Smyth vs. Pillsbury Co.* (1996), in which an employee brought suit against his employer for wrongful discharge. The employee had been fired after company executives reviewed the contents of his e-mail messages and found them to contain offensive references toward certain company personnel. He had sent these messages to his supervisor in the knowledge that company policy held that all e-mail communications would remain private and confidential. The plaintiff argued that his termination was against public policy as a violation of his common law right to privacy. The court analyzed his claim under the definition of intrusion upon seclusion and found, first, that the plaintiff could not have a reasonable expectation of privacy in e-mail communications voluntarily made to his supervisor over the company e-mail system. Second, even if he was determined to have a reasonable expectation of privacy in the contents of his e-mail messages, the court would not consider his interception of those communications to be a substantial and highly offensive invasion of privacy, particularly since the e-mail system belonged to the company. The court concluded by adding that any privacy interest of the plaintiff was outweighed by the employer's interest in preventing inappropriate and unprofessional comments over its e-mail system.

As the only cases so far applying common law invasion of privacy to tort e-mail monitoring, *Bourke* and *Smyth* offer a grim outlook for e-mail privacy in the workplace. The cases suggest that courts will provide a very narrow reading of employees' reasonable expectation of privacy. *Bourke* holds that maintaining a personal password to access the e-mail system does not give rise to an objectively reasonable expectation of privacy. *Smyth* indicates that even an employer's stated policy that employee e-mail is private and confidential will not necessarily give rise to an objectively reasonable expectation of privacy. Thus, the current state of common law with respect to e-mail monitoring clearly favors employers.

"As the only cases so far applying common law invasion of privacy to tort e-mail monitoring, Bourke and Smyth offer a grim outlook for e-mail privacy in the workplace."

It should also be noted that a well-written e-mail policy may not only immunize an employer from liability under the ECPA, but may also immunize it from tort liability for invasion of privacy. In fact, the two cases above strongly support the proposition that a well-written e-mail

policy will be sufficient to render unreasonable any expectation of privacy.

New Legislation

The weaknesses of the ECPA combined with increased employee awareness and sensitivity to privacy in the workplace have led to the proposal of new legislation to address the issue of monitoring electronic communications in the workplace. In 1991, the Privacy for Consumers and Workers Act (PCWA) was introduced in Congress, addressing issues of private-sector employee privacy and preserving employee rights. Its provisions would allow a company to monitor employees' e-mail and use the information against them to some extent. However, prior to monitoring, the company would be obligated to inform the employees of the potential, form, and scope of the monitoring, as well as what the data collected might be used for.

The original version of the PCWA failed to pass through Congress. At present, a revised version is still being debated in congressional committee. Meanwhile, the debate over private-sector workplace privacy has been stirred up. The proposal of the PCWA has served to highlight the need for further legislation—beyond the scope of the ECPA—to protect employees' rights to privacy.

BUSINESS RAMIFICATIONS

Driven by the desire to increase productivity and minimize liability, employers have adopted monitoring techniques in an effort to control all aspects of the workplace. They can provide other justifications as well for maintaining these invasive practices, such as the need to evaluate worker performance more efficiently, the need to deter or uncover employee wrongdoing and dishonesty, and even the need to limit tort liability under the respondent superior doctrine.

In 1998, U.S. industry spent half a trillion dollars on computer hardware and software, communications, and training and support. Many companies are now grappling with employees using that technology for purely personal transactions during business hours. This abuse has lowered companies' return on their technological investments. Its cost to employers can only be estimated, but all would agree it is substantial.

Examples of such employee abuse abound. Recently, Salomon Smith Barney terminated two high-ranking stock analysts for using company e-mail systems to share pornography. An analysis of computer logs by Neilsen Media Research found that employees at IBM and Apple together visited Penthouse Magazine's Web site almost 13,000 times in a single month in 1996, using up the equivalent of almost 350 eight-hour days. Another study by SurfWatch Software, a Web filtering company based in Los Altos, California, found that 24 percent of the on-line traffic at the companies surveyed was not work-related. Sites most commonly visited, reports GaroFalo (1998), were general news, sex, investments, entertainment, and sports. Thus, employers have a legitimate interest in workplace monitoring if they want to limit inappropriate use of company time and maintain or increase productivity.

When it comes to protecting themselves against liability, employers are insisting on the right to monitor communications. They rightfully cite their legitimate interest in running an efficient business and in hiring and retaining honest and productive employees who will perform their jobs in a safe manner. And they fear claims asserting a hostile workplace environment, or harassment lawsuits by workers who happen upon offensive messages. Industry leaders, including Citibank and Morgan Stanley, have been sued by employees over the content of e-mail messages. Recently, a federal court in New York held that a class action race discrimination suit seeking damages of $60 million could proceed against Morgan Stanley, a large Wall Street brokerage firm. The lawsuit stemmed in part from the alleged repeated dissemination of a racist e-mail message through the company's computer system. More and more, cases of sexual harassment and discrimination include allegations that the company e-mail systems were used to transmit inappropriate or offensive material.

Viewing the privacy component of new technology from a different angle, it is possible that increased employee privacy may result in a more efficient workplace. It sends a positive message from the employer to the employees, implicitly trusting them to be responsible for their time and productivity. Such a message could fortify the work relationship between a firm and its workers and infuse personal dignity into the workplace. In contrast, an employer who monitors the workplace daily and is privy to all internal communications may create a workplace filled with distrust. Employees who do not trust their employer have a lower incentive to be efficient, resourceful, and productive.

ETHICAL IMPLICATIONS

There are two main ethical issues regarding privacy in the workplace: employee abuse of company resources and employer abuse of workers' privacy rights. The latter hinges on the notions of human dignity and trust.

In a study reported by GaroFalo, nearly half of the 726 employees surveyed acknowledged

that they had engaged in unethical actions using their employers' technology during the previous year. Further, more than one-fourth of those responding stated that they had committed at least one highly unethical or illegal act, including copying company software for home use, using office equipment to search for other jobs, accessing private computer files without permission, visiting pornographic Web sites using office equipment, or sabotaging systems or data of former employers and coworkers.

Americans' respect for privacy has helped creativity and individuality flourish. So the negative effects of reduced individual privacy rights go far beyond simple embarrassment. Loss of privacy often induces conformity to perceived societal norms in order to safeguard personal and professional interests. American culture has been built on diversity and the willingness to accept challenges that test people's creativity. Yet these traits that helped mold our country will suffer if conformity, not privacy, is considered the principle value. Perhaps worst of all, inroads into privacy inhibit personal autonomy and thus individual freedom.

Of course, in addition to the fundamental interest individuals have invested in privacy, they also have a need to obtain and maintain employment. Some employee monitoring is always necessary. Tracking productivity and attendance is done in many, if not most, organizations. It is, however, the seemingly secretive or unexpected nature of certain types of monitoring or surveillance that tend to engender most of the bad feelings that may lead to actionable invasion of privacy claims.

Employers have an obligation to respect the privacy of their employees as well as inform them of monitoring intentions and policies. In addition to buttressing a firm's right to protect its interests, implementing a formal e-mail policy would also reflect an ethical responsibility to protect employees' privacy. One approach is to create a sign-on disclaimer that defines the degree and scope of privacy allowed and reiterates the fact that e-mail is company-owned property. Moreover, employees should be informed that their e-mail communications may be monitored at any time by the company and that, by using the e-mail system, the employee is consenting to be monitored. Finally, users of the e-mail system should be told explicitly not to send inappropriate messages, or they could face disciplinary consequences, up to and including the possibility of discharge.

As workplace technology continues to improve and become more prevalent and more available to employees, so too will the opportunities for employee abuse and, concurrently, the avenues available to firms to monitor and control employee activities. Companies must, however, be cognizant of the impact such activities have on the morale of the employees, who feel that their rights are being trampled. They must also beware the possible legal ramifications of overreaching. Employers who engage in monitoring, surveillance, or searches should do so only pursuant to a well-written policy that has been distributed in advance to all employees. Moreover, any such monitoring should be reasonable in nature and strictly for business purposes.

To best address the issue of workplace privacy in light of evolving technology, new federal legislation should be enacted, balancing the rights of employees to privacy with the rights currently afforded to employers. New legislation will also serve to heighten employee awareness of companies' policies regarding the use of workplace technology. The time to embark on such a course of action was yesterday. ❐

References

H. Chase and C.R. Ducat, *The Constitution and What It Means Today,* 13th ed. (Princeton, NJ: Princeton University Press, 1978).

B. Cole-Gomolski, "The Lethal Sting of Forgotten Mail," *Computerworld,* September 8, 1997, pp. 1, 117.

R. Dixon, "Windows Nine to Five: *Smyth v. Pillsbury* and the Scope of an Employee's Right of Privacy in Employer Communications," *Virginia Journal of Law and Technology,* Fall 1997, pp. 1-26.

S.S. Fader, "Want Some Privacy? Stay at Home," *Chicago Tribune,* May 28, 1998, pp. 1, 3.

W.S. Galkin, "Database Protection: Just the Facts," *The Maryland Bar Journal,* May-June 1993, p. 40.

B. GaroFalo, "Sharing a Middle Ground With Big Brother," *Connecticut Law Tribune,* May 18, 1998, p. 1.

W.S. Hubbartt, *The New Battle Over Workplace Privacy* (New York: AMACOM, 1998).

K.P. Kopp, "Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy," *Seton Hall Constitutional Law Journal,* Summer 1998, pp. 1-30.

A. Rodriguez, "All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace," *Emory Law Journal,* Fall 1998, p. 1439.

P. Schnaitman, "Building a Community Through Workplace E-Mail: The New Privacy Frontier," *Michigan Telecommunication and Technology Law Review,* 1998-99, p. 177.

J. Sipior, B.T. Ward, and S.M. Rainone, "Ethical Management of Employee E-Mail Privacy," *Information Systems Management,* Winter 1998, pp. 41-47.

S. Stipe, "Establish E-Mail Policy to Avoid Legal Pitfalls," *Best's Review,* July 1996, pp. 102-103.

S.E. Wilborn, "Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace," *Georgia Law Review,* Spring 1998, pp. 825-887.

N. Wingfield, "More Companies Monitor Employees' E-mail," *Wall Street Journal,* December 2, 1999, p. B5.

Kenneth A. Kovach is a professor of management at George Mason University in Fairfax, Virginia. **Sandra J. Conner, Tamar Livneh, Kevin M. Scallan,** and **Roy L. Schwartz** are MBA students at the University of Maryland, College Park, Maryland.