BY G. DARYL NORD, TIPTON F. MCCUBBINS, AND JERETTA HORN NORD

E-Monitoring in the Workplace: PRIVACY, LEGISLATION, AND SURVEILLANCE SOFTWARE

Protecting the corporation while respecting employee privacy—an old puzzle made more complex with new software.

"Through advanced computer technology, employers can now continuously monitor employees' actions without the employee even knowing he or she is being 'watched.' The computer's eye is unblinking and ever-present. Sophisticated software allows every minute of the day to be recorded and evaluated [1]."

Increasingly, personnel in institutions worldwide use email and the Internet on a daily basis at work. This daily reliance and dependency on technology has created new issues with respect to employee privacy in the workplace and has added new stress to the employer-employee relationship. Employee privacy, long considered a basic right, is often taken for granted by employees. However, as a result of technological monitoring, this view may be naïve.

According to the annual survey, *Workplace Monitoring and Surveillance Survey 2001* conducted by the American Management Association, more than three-quarters of all major U.S. firms (nearly double the 1997 survey results) are recording and/or reviewing the email messages, telephone calls, Internet connections, and computer files of their employees. Workplace monitoring has existed for a long time in one form or another and will undoubtedly continue to proliferate and become increasingly sophisticated as technology advances. This article examines the employer/employee workplace privacy relationship, identifies the existing federal and state law governing workplace privacy, and discusses the rapidly developing monitoring software market.

WORKPLACE PRIVACY

Most U.S. citizens are accustomed to the expectation of privacy. Privacy, as defined by the Merriam-Webster dictionary is a: the quality or state of being apart from company or observation; b: freedom from unauthorized intrusion <one's right to *privacy*>. But in the workplace, to what degree can workers expect privacy and protection from observation and unauthorized intrusion? Workers may sometimes expect they have the same privacy rights at the office as they have at home. Others may assume that since they have an account number and password on their software and email system their individual privacy is protected and secure.

ILLUSTRATION BY RICHARD DOWNS

Do you know anyone who occasionally takes a moment out of his or her day to check a stock quote, sports score, or movie listing online at work? As of January 2002, approximately 55 million U.S. adults accessed the Internet at work, up from 43 million in March 2000. Fifty-five percent of those with Internet access at work went online on a typical day in 2001, compared to 50% in 2000, and many were going online more frequently throughout the day than they had in 2001 [10]. More than 72% of Internet users do more than just surf the Web. Popular Internet activities include instant messaging, downloading music, and watching video clips [9]. In another Internet work-related study, Yankelovich Partners discovered that 62% of workers go online at work for personal reasons at least once a day, while about 20% do so 10 or more times a day. In a 2002 study by the Computer Security Institute (CSI), 78% of polled enterprises reported employee abuse of Internet access privileges by workers, including downloading pirated software or pornography, shopping on the Internet, and inappropriate use of email systems. These studies readily show the escalating magnitude of non-work related Internet use at work.

	1999	2000	2001	2005
Storage and review of computer files	21.4%	30.8%	36.1%	50%
Storage and review of email messages	27%	38.1%	46.5%	55%
Monitoring Internet connections	NA	54.1%	62.8%	76%

Table 1. Survey results by AMA on employee monitoring.

Employers want to make sure their employees are using company time productively and not creating a legal liability for their business as a result of harassing or offensive communications. A recent study revealed that 10% of U.S. companies have received subpoenas resulting from employee email [5]. In addition, employers have security concerns relating to the intentional or accidental sending of sensitive data via email attachments as well as the ongoing concern of viruses entering the business from outside communications. Consequently, employers are monitoring employee's computer and Internet access to a greater degree than in the past. As illustrated in Table 1, the American Management Association surveys conducted from 1999 to 2001 and again in 2005, exposed the growing trend of employer monitoring of employees' computer files, email messaging, and Internet connections [2].

According to another recent AMA survey, the 2003 E-mail Rules, Policies and Practices Survey, over half (52%) of employers monitor email. Three-fourths of the 1,100 employers surveyed have put written email policies in place. And 22% have terminated an employee for violating email policy [3].

Federal Privacy Legislation in the Workplace

Most U.S.-based employees assume they have a constitutional right to privacy. However, constitutional rights to privacy are generally inferred through the U.S. Constitution's Fourth Amendment's rights to freedom from unreasonable search and seizure. These freedoms usually apply only to state actions. In an employment context, state actions are fairly narrowly limited to protecting federal, state, and municipal employees. Private-sector employees must look elsewhere for protection. Possible sources for such protection from employer snooping include federal legislation and state common law tort actions such as invasion of privacy [4].

The primary piece of federal legislation suggesting employee privacy interest is the Electronic Communications Privacy Act (ECPA). However, there are three exceptions under the ECPA that effectively

Workplace monitoring has existed for a long time in one form or another and will undoubtedly continue to proliferate and become increasingly sophisticated as technology advances.

eliminate any substantial expectation of privacy an employee might have with respect to his/her employer.

The first of the ECPA exceptions is the "provider exception." If an employer actually owns and is providing the telephone, email, or Internet services to the employee being monitored, there is little doubt that the employer is protected from employee privacy claims. However, if the employer is merely providing email services through a third-party Internet provider, it is not as clear that the employer would enjoy the same protection. Nevertheless, given the fact the employer is "providing" the provider, coupled with the generous interpretation that most courts have granted employers, there is good reason to believe that even these providers of providers would enjoy protection from employee privacy suits [7].

The second exception is the "ordinary course of business" exception. It really provides an exception to the definition of an electronic device, and therefore excludes the employer's monitoring from the ECPA and the employee protections provided therein. Under this exception the employer may monitor employee communications to ensure such legitimate business objectives as assuring quality control, preventing sexual harassment, and preventing unauthorized use of equipment, such as excessive telephone or email usage.

However, the "course of business" language also implies a limitation on the extent of monitoring in the event the employer discovers he has accessed a personal conversation. In monitoring telephone conversations it is well established that employers can continue to listen only for so long as it takes to determine the conversation is in fact personal. At that point, the employer must cease the surveillance. The case setting the standard for this limitation is a 1983 case dealing with the use of the telephone. A thorough examination of the standard as it applies to email usage has not yet occurred, but a similar application should probably be expected. However, at least one case has suggested that no monitoring of an employee's personal email may be allowed without prior notification [8].

The third exception is the "consent" exception. If at least one party to the communication is either the party who intercepts the communication or gives consent to the interception then the ECPA has not been violated. The "consent" exception apparently applies even when the sender of the intercepted communication has been assured that all email communications would remain confidential and privileged. In *Smyth v. The Pillsbury Company*, Smyth sent his supervisor emails that contained inappropriate and unprofessional comments from Smyth's home computer. The supervisor received the email over Pillsbury's email system. The email included such statements such as "kill the backstabbing ..." and referred to the company's holiday party as the "Jim Jones Koolaid affair." At a later date the company intercepted these email messages and terminated Smyth's employment based upon their content.

The workplace end user types any keystroke in any window on his/her remote PC, that text appears on the network administrator's screen in real time or archived to a corporate server.
Typed text that is monitored may include email messages, online chat conversations, documents, passwords and all other keystrokes.
The network administrator can view the actual screen of the workplace desktops being monitored.
Internet usage can be monitored in real time and a log file recording of all Internet activity can be made.
A spy module can see and list software running on the remote PC and can view in real time the software applications and run executions.
A record and activity log for all workstations on the local or shared network location can be produced.
Monitoring software provides the ability to take snapshots of a remote PC screen or active window in specified time intervals and save them on the local or shared network location.
The workplace user's system can be turned off, restarted, and actually logged completely off the network.
The network administrator can run programs and execute commands on remote computers, open Web pages or documents, send instant messages for remote users, and terminate remote processes.
Files can be readily copied including logs and screenshots from the desktop computers. The administrator can have the same file access permissions, as a current user has on the workplace computer.
Multiple employee computers can simultaneously be monitored from a single workstation in the LAN.
Workplace surveillance software that runs on monitored computers is hidden and difficult for an employee to locate or even know that the software is present and monitoring their every keystroke. The monitoring software usually cannot be terminated without the network administrator's permission.

Table 2. Surveillance capabilities of monitoring software on the market today.

Although the court did not explain exactly how the interception took place, the email messages were apparently retrieved from storage with the supervisor's consent. As a result of the consent, even the prior promise of confidentiality did not provide the employee with privacy protection.

State Privacy Case Law

The common law tort of invasion of privacy is recognized by most states. The Restatement (Second) of Torts §652B defines invasion of privacy as: "...intentionally intruding, physically or otherwise, upon the solitude or seclusion of another..., if the

Along with the ever-increasing exploitation of technology in the workplace has come the capability for employers to see and measure nearly every aspect of company usage.

intrusion would be highly offensive to a reasonable person." Employees have tried to use this tort as a protection for privacy in the workplace. Although it shows some potential for privacy protection, it has generally stumbled over two problems. The first is that the employee must have a reasonable expectation of privacy, and the second is that the intrusion would be highly offensive to the reasonable person.

In *McLaren v. Microsoft* (1999), Microsoft made available to McLaren, as part of his employment, use of an email system owned and administered by Microsoft. McLaren had the right and ability to store email he received either in the server-based "inbox" or in a "personal folder" protected by a personal store password. As part of a harassment investigation, Microsoft decrypted McLaren's personal store password and broke into his personal folder even though it had been specifically requested by McLaren not to do so.

McLaren argued that the password-protected personal folder was basically the same as a locked storage locker provided by a company for employees to store personal items in while at work. It has long been accepted that employees have a legitimate expectation of privacy with regard to such lockers. However, the court rejected this argument. It stated that because the email was first received and stored in the "inbox," which was subject to inspection, McLaren could have no expectation of privacy simply by moving it to a protected folder. How this is different from a telephone call that can only be monitored long enough to determine if it is of a business or personal nature the court did not explain. True, in this case, the fact that the email messages were pertinent to a harassment investigation would make them subject to legitimate business scrutiny. However, the court did not seem to rely on this fact in declaring a blanket open season on email monitoring. Second, although it is possible to distinguish between illicit information being carried through public space from the front door of a business to an employee's locked storage locker and an email message sitting in an inbox before being transferred to a protected personal folder, such distinctions are not so obvious as to deny a need for recognition. However the court seemed sufficiently confident in its analysis that it did not address the issue.

In determining that the intrusion was not highly offensive, the court properly recognized the importance of whether the intrusion was justified. The fact that McLaren was under investigation, and that he had notified Microsoft that the email was relevant to that investigation, clearly support the court's finding that Microsoft's actions were justified. Therefore, they were not highly offensive even though the actions had been specifically forbidden by McLaren and led to his dismissal.

Company Electronic Communications Policy

In a case [11] in which the California Appellant Court ruled in favor of the employer strictly on the basis of a signed electronic communications policy, the court stated that at a minimum the policy should contain a statement that:

1. Electronic communication facilities provided by the company are owned by the company and should be used solely for company business.
2. The company will monitor all employee Internet and email usage. It should state who may review the information, the purposes for which the information may be used, and that the information may be stored on a separate computer [6, 7].
3. The company will keep copies of the Internet and email passwords.
4. The existence of a separate password is not an assurance of the confidentiality of the communi-

cation or other "protected" material.

5. The sending of any discriminatory, offensive, or unprofessional message or content is strictly prohibited.
6. The accessing of any Internet site that contains offensive of discriminatory content is prohibited.
7. The posting of personal opinions on the Internet using the company's access is strictly prohibited. This is particularly true of, but not limited to, opinions that are political or discriminatory in nature.
8. Although not included in the court's list, the policy should clearly state potential repercussions to the employee for violating the policy [4].

Legally, these requirements are considered minimum standards that a sound policy should meet. They should be clear and unequivocal, and they should be read and signed by each employee. However, the employer should also remain aware of the employee's normal human desire for reasonable amounts of privacy. Therefore the employer should try to minimize unnecessary intrusion into this privacy expectation in order to reduce the negative impact on employee morale.

Monitoring Software

Along with the ever-increasing exploitation of technology in the workplace has come the capability for employers to see and measure nearly every aspect of company computer usage. The dilemma that employers must resolve is how to balance the obvious benefits of employee use of technological tools with the risks inherent in providing those tools to employees. As stated earlier, many employers have sought to achieve this balance by electronically monitoring the use that their employees make of email, the Internet, and other computer-related activities.

Monitoring software allows employers to see, measure, and manage employees' computer systems, monitors, disks, software, email, and Web and Internet access. The software can automatically archive all collected information into a corporate network server for review at a later time. The list in Table 2 illustrates the many capabilities of typical monitoring software readily available on the market today by companies such as Spectorsoft and DynaComm.

Conclusion

E-monitoring and employee workplace privacy are issues that will continue to present questions and problems for some time to come. In addition, it looks as if there will be ongoing efforts to balance employee workplace privacy with the need for employers to manage and protect company resources from non-productive, non-work related activities. Federal and state legislation governing monitoring and workplace privacy will undoubtedly continue to evolve and be tested in the court systems.

There are many legitimate reasons for organizations to want to know what is occurring on their computer systems. Those reasons range from workplace harassment, to loss of productivity, and even to company sabotage. Therefore, it is easy to understand why it would be prudent for companies to have such a strong incentive to find a healthy balance between employee privacy rights and organizational concerns. C

References

1. American Civil Liberties Union (ACLU). Workplace Rights on Electronic Monitoring, ACLU online archives; archive.aclu.org/issues/worker/legkit2.html.
2. American Management Association, AMA Research: Workplace Monitoring and Surveillance, 1999, 2000, 2001 and 2005; www.amanet.org/research/archive_2001_1999.htm.
3. American Management Association, Survey on Workplace E-Mail Reveals Disasters in the Making, May 28, 2003; www.amanet.org/press/amanews/Email_Survey2003.htm.
4. Bloom, E., Schachter, M., and Steelman, E. Justice in a Changing World: Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety. 29 Wm. Mitchell L. Rev. 897 (2003).
5. Crimmins, J. Even federal judges come under surveillance when online. *Chicago Daily Law Bulletin 147*, 159 (Aug. 14, 2001).
6. *Deal v. Spears*, 980 F.2d 1153, 1155-1157 (8th Cir. 1992).
7. DiLuzio, S. Workplace E-Mail: It's Not as Private as You Might Think. 25 Del. J. Corp. L. 741 (2000).
8. Kopp, K. Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy. 8 Seaton Hall Const. L. J. 861 (1998).
9. Neilson//NetRankings, U.S. Online Population Internet Use. (Dec. 18, 2002); www.nielsen-netratings.com/pr/pr_021218.pdf.
10. Pew Internet & American Life, Getting Serious Online: As Americans Gain Experience, They Use the Web More at Work, Write Emails with More Significant Content, Perform More Online Transactions, and Pursue More Serious Activities, (Mar. 3, 2002); www.pewinternet.org/reports/toc.asp?Report=55.
11. *TBG Insurance Services Corporation v. The Superior Court of Los Angeles Co.*; Robert Zieminski, Real Party in Interest, 96 Cal. App. 4th 443; 117 Cal. Rptr. 2d 155 (Cal. App. 2002).

G. Daryl Nord (daryl.nord@okstate.edu) is a professor of Management Science & Information Systems in the William S. Spears School of Business, at Oklahoma State University, Stillwater, OK.
Tipton F. McCubbins (tipton.mccubbins@okstate.edu) is an associate professor of Legal Studies in Business in the William S. Spears School of Business, at Oklahoma State University, Stillwater, OK.
Jeretta Horn Nord (jeretta.nord@okstate.edu) is a professor of Management Science & Information Systems and Associate Dean for Undergraduate Programs in the William S. Spears School of Business, at Oklahoma State University, Stillwater, OK.