WHO'S READING YOUR OFFICE E-MAIL?

Is That Legal?

By Chauncey M. DePree, Jr., and Rebecca K. Jude

YESTERDAY, as you sat working at your desk, you checked your e-mail and spotted a note from a friend. The message was an off-color joke complete with graphic illustration. Sure, some stick-in-the-mud might find it offensive, but it was awfully funny. So, without thinking, you clicked on the forward button, typed in an e-mail address or two or three, and hit the send button. No big deal, right?

You don't give the e-mail another thought until this morning when a somber supervisor invites you to her office. She hands you a letter of reprimand along with a copy of the e-mail. She tells you that as a matter of office policy, employee e-mails are monitored. Copies are placed in your file, and, in the event it happens again, she warns that you'll receive a termination letter.

It simply never occurred to you that someone might be monitoring your e-mail. What about your right to privacy?

WHAT HAPPENED TO PRIVACY?

As an employee, the idea of being monitored may trouble you. As an employer, the idea of monitoring employees may be equally distasteful. The right to privacy is so thoroughly ingrained in most of us that we take it for granted—especially in a peaceful environment when we're sitting alone, typing into a computer. We may be lulled into a false sense of isolation and freedom from observation. But even if the technology is available, aren't there simply too many e-mails and too much Internet use to review effectively? After all, the Internet is so big and

so anonymous. No one can really track everybody's e-mail or Internet surfing. Besides, it's probably an invasion of privacy and illegal.

Wrong on both counts. To quote Scott McNealy, CEO of Sun Microsystems, on the issue of Internet privacy: "You have zero privacy anyway. Get over it." McNealy's rather abrupt observation and admonition are particularly true in the work environment.

The simple fact is that monitoring employee e-mail and Internet usage is legal under almost all circumstances. As a general rule, when an employee enters the workplace, an employer may monitor and record communications, including e-mail and Internet use, without any notice to the employee. In *Fraser v. Nationwide Mutual Insurance Co.*, 352 F. 3d 107 (3rd Cir. 2003), the court specifically held that The Electronic Communications Privacy Act, 18 U.S.C.§2701, didn't apply to an employer's search of e-mail stored on its own system.

But in some instances, simple facts tend to beget complicated, counterintuitive consequences. For example, an employer repeatedly assured its employees that e-mail communications would remain confidential. As it turned out, the assurance wasn't a guarantee that the employees' e-mails wouldn't be used as a basis for discharge. In *Smyth v. The Pillsbury Company*, 914 F. Supp. 97 (ED Pa. 1996), a supervisor e-mailed inappropriate comments to an employee at home, and the employee responded in kind. The e-mails were communicated over the company system. Regardless of the company's assurances, the employee was terminated for communicating "inappropriate and unprofessional comments" via the company system. The Court held that "once plaintiff communicated the alleged unprofessional comments to a second person over the e-mail system that was apparently utilized by the entire company, any reasonable expectation of privacy was lost."

Employee e-mail habits have developed over time, but, as the *Pillsbury* decision exemplifies, employers' practices also can change—sometimes quickly and unpredictably. The Pillsbury case wouldn't be the last surprise for employees. Employers can review e-mail at any time and with lightning speed. Dow Chemical took a "snapshot" of a day's worth of employee e-mails and then systematically sorted through them. Some 254 employees had saved, filed, or sent sexually related, violent, and other inappropriate e-mails. The actual participation and involvement of the employees varied considerably. Dow created a set of criteria so that discipline taken, if any, could be based on each employee's participation. The criteria included offensiveness; what the employee did with the material, such as circulating the materials within Dow; and the frequency of the conduct. Dow discharged 20 employees and disciplined others. The court, although recognizing that Dow was probably employing a union-busting tactic, upheld the company's review and use of its employees' e-mail (*Dow Chemical v. Local No. 564, Operating Engineers*, 246 F. Supp. 2d 602 (SD Texas, 2002).

IS MONITORING E-MAIL AND INTERNET USE NECESSARY?

Despite the near cultural aversion to intruding on communications, growing numbers of companies and managers record, review, and monitor telephone and computer activities of their employees. According to the American Management Association (AMA) 2005 Electronic Monitoring & Surveillance Survey, 76% of employers monitor website connections, "26% have fired workers for misusing the Internet," and "another 25% have terminated employees for e-mail misuse." Inexpensive software packages facilitate these decisions, and the overriding reason is compelling—it has become a business necessity.

An inescapable consequence of employee e-mail and Internet use is that the employer is responsible for illegal, discriminatory, or offensive communications that are transmitted over the system or viewed by others from a company computer screen. Sexually explicit, graphically violent, or racially inappropriate websites open to view by co-workers may be used to support claims of discriminatory behavior or a hostile work environment. E-mails containing such inappropriate materials that are circulated around the office or forwarded to others have the same effect.

But so there's no misunderstanding, employers and managers can get into just as much trouble with their e-mail as employees. E-mails sent by managers can be used by employees to prove claims of corporate misconduct. For example, the characterization of an employee as "ready for the bone yard" may be evidence of age discrimination. The simple truth is that e-mails containing potentially libelous or defamatory content should *not* be sent or forwarded—even internally. Not only can they easily get away from managers with a click of a button, but they also may become—in a stored capacity on the server or archive—the target of discovery in litigation.

Because e-mails can seem so informal, managers and employees are more likely to say things in them they would never put in a letter. Unlike letters, e-mails can be forwarded over and over to thousands of people with the touch of a button. Impulsive and thoughtless comments can travel

the world over. Often overlooked is the liability with regard to foreign laws. Because e-mails can be transmitted anywhere and may then be forwarded practically *ad infinitum*, an employer may be responsible for content based on the laws of the country in which the e-mail ultimately arrives. Electronic communications originating in the company office may have far-ranging legal consequences.

AN EASY PREDICTION AND ANOTHER SURPRISE

Some potential liabilities are much better known and may occur with considerable frequency. For example, an employee might use office computers to wrongfully appropriate other people's intellectual property from the Internet, leaving the employer responsible. One of the most popular forms of this activity is file sharing—downloading copyrighted music or movies without payment. Or an employee might copy and paste copyrighted material from someone else's website onto the employer's without the knowledge or consent of any manager or supervisor. The company may be responsible for the copyright infringement.

Other kinds of e-mail-facilitated problems might not be easily anticipated. For example, an employee can enter into a contract with the click of a mouse. This was our firm's first e-mail surprise. An employee took it upon himself to purchase CDs containing copies of documents that we already had in our possession. It was easy. An e-mail arrived asking if he would be willing to share the cost of obtaining copies of documents. All he had to do was return an e-mail agreeing to participate in the project. Seemingly out of the blue, at least from our perspective, a half dozen CDs and an invoice for several thousand dollars arrived at our office. There was no correspondence in the files authorizing the purchase. Ultimately, though, we found a brief e-mail from our employee responding to the inquiry. The reply e-mail simply said "count us in." Of course, the company that provided the service wanted its money. After all, they had spent time and effort preparing the materials for us. We were stuck. If our office had monitored e-mails, we could have caught this and stopped the expensive and wasteful process before the vendor incurred its costs.

FROM TOP TO BOTTOM LINE

Even when a company gets lucky and avoids civil or contractual liability, employees will still take time for personal communications, e-mails, and Internet surfing instead of working. This could cost the company a fortune in lost productivity and lost dollars. Time away from work also translates to poor client service. Poor service may lose clients. Consequently, as unappealing as it is, monitoring employee communications is increasingly viewed as a business necessity.

For our firm, a good place to start was to develop a policy to educate employees in the use of company e-mail and the Internet. We believed, as do other employers, that to avoid any potential gray areas in the law, and in the interest of fairness, employers should advise managers and employees of e-mail or Internet monitoring as part of their employment agreement, and it should be included in the employee handbook. We breathed a sigh of relief after we disseminated the policy to all employees and confirmed that everyone understood the importance of compliance.

We weren't so naïve as to believe it would solve our Internet and e-mail problems, but we had no idea just how difficult it would be to change habits. As unbelievable as it may sound, the very next day after the Internet and e-mail policy was communicated, it was completely ignored by a professional employee. He thoughtlessly e-mailed his latest "joke" far and wide, even though it could easily be construed not only as racist but salacious as well. It was forwarded as cavalierly as if he had never read the policy or studied the law. And that's right, he is a lawyer! ■

Chauncey M. DePree, Jr., DBA, is a professor in the School of Accounting and Information Systems at the University of Southern Mississippi, Hattiesburg, Miss. You can contact him at m.depree@usm.edu.

Rebecca K. Jude, Esq., is a principal at the law firm, Jude & Jude PLLC in Hattiesburg, Miss. You can contact her at katejude@judelawfirm.com.

MORE ON PRIVACY

The Privacy Rights Clearinghouse
This nonprofit consumer information site has a number of fact sheets concerned with workplace and Internet privacy: www.privacyrights.org/netprivacy.htm#factsheets.

The Electronic Frontier Foundation (EFF)
A nonprofit advocacy and legal organization based in San Francisco that's dedicated to preserving free speech rights. Two sections of its website look at e-mail, privacy, and the law: www.eff.org/Privacy/Email_Internet_Web and www.eff.org/legal (general legal issues in cyberspace).