Establishing an Electronic Communications Policy

Why you (and your clients) shouldn't be without one.

by Andrea J. Bernard

Developments in electronic communications over the past 15 years, and the attendant changes they have brought to the work environment, are staggering: e-mail has taken the place of interoffice memos; voice mail has replaced the telephone slip; fax machines have replaced the mail; and the Internet has replaced the library.In the United States alone, industry analysts estimate that 122 million people have access to the Internet at work. This number is predicted to rise as high as 272 million by 2004. Like many advances, however, the computer can be both a tremendous asset and a destructive force.

"Cyberslacking"

Cruising the net has become a 9-to-5 hobby for many employees. Surveys show that as many as 35 percent of employees with Internet access regularly surf recreational sites during office hours, often for up to five hours per day. Top Internet distractions include news sites, shopping, and, perhaps most disconcerting for employers, job hunting. True net-surfers can even find custom-designed, self-proclaimed cyberslacking websites such as Gamesville.com, DonsBossPage.com, and IShouldBeWorking.com, where visitors will find distractions ranging from games to chat rooms to advice from "expert" cyberslackers on how best to surf the Internet at work without being caught.

The Internet also offers disgruntled employees the perfect forum to air complaints. Specialized websites exist where employees can post stories and complaints about their employers or co-employees. Employees can also anonymously post false statements about their company over the Internet. And perhaps most harmful, employees can use the Internet to disseminate truthful information about an employer that is nonetheless very harmful such as public disclosures of company trade secrets or other proprietary information.

Litigation and Harassment Risks

Many employers are finding that sloppy use of e-mail and the Internet is causing and exacerbating litigation. In particular, the Internet and electronic mail systems present a new twist on the age-old problem of workplace harassment. It is increasingly common for evidence of sexual, racial, or other forms of harassment to be found in electronic communications containing graphic images, sexually explicit jokes, or other derogatory and offensive content. And, human nature being what it is, employees will often send things in electronic form that they wouldn't dare say to a recipient's face. Unlike verbal comments, electronic communications can create a permanent record of evidence. Hitting the "delete" button often does not eliminate an e-mail message; it simply sends it to a new storage place. Creative litigators in all kinds of cases are becoming increasingly aggressive about accessing the opposition's computers and other electronically stored data to mine for evidence that might be beneficial.

Strain on Company Computer Systems

Perhaps the most obvious "cost" associated with personal e-mailing and Internet surfing is the undue pressure it can place on a company's computer systems and network. More and more web retailers are producing continuous stream video and live "webcasts" that impose a tremendous strain on networks. For example, in May 2000, Victoria's Secret webcast an on-line fashion show at 3:00 p.m. Over two million people tuned in. Experts conclude that streaming just that one webcast was the functional equivalent of downloading the entire Encyclopedia Britannica onto an employee's network.

Union Issues

As the U.S. economy moves further away from a traditional manufacturing base and closer to a technology base, unions are continuously looking for new ways to solicit membership. Organizing drives have been strengthened through the use of the Internet, and the use of websites and e-mail are giving unions ready access to millions of workers. What's more, the availability of e-mail in the workplace has given creative employees and unions another channel for protected and concerted communications.

"Surveys show surf recreational

Perhaps the most well-known case in this regard is *Timekeeping Systems, Inc*, 323 NLRB 244 (1997), in which a Chief Operations Officer e-mailed a proposed company vacation policy to all employees and solicited comments. An employee accepted the solicitation, and responded with an unfavorable review of the plan. Unfortunately, the employee also took it upon himself to respond in an arguably flippant and discourteous fashion, and to copy the reply message to his coworkers.

The COO responded by ordering the employee to either publicly retract his message or be terminated. The employee elected the latter, and pursued his case with the NLRB. The NLRB found that the employee's communication was a protected concerted activity that was immune from reprisal under the National Labor Relations Act.

Disclosure of Confidential Information and Trade Secrets

Growth in the use of computers, e-mail, and the Internet has made it easier for competitors to steal information from one another and harder to keep confidential information from intentional or accidental disclosure to the public or competitors. Employees frequently change jobs, leaving open the risk that they will take their employer's trade secrets and confidential information along with them. Theft of trade secrets may occur with an employee's deliberate and active assistance or even through an employee's innocent and inadvertent mistakes. Either way, the harm is the same.

Fast Facts:

- An employer's most effective tool against inappropriate computer use and abuse is a comprehensive and uniformly distributed electronic communications policy.
- Growth in the use of computers, e-mail, and the Internet has made it easier for competitors to steal information from one another and harder to keep confidential information from intentional or accidental disclosure to the public or competitors.
- Internet filtering software allows employers to monitor where employees go on the Internet and how much time they spend there.

that as many as 35 percent of employees with Internet access regularly sites during office hours, often for up to five hours per day."

Electronic Communications Policies

An employer's most effective tool against inappropriate computer use and abuse is a comprehensive and uniformly distributed electronic communications policy. Such policies, if properly drafted, clearly define the employer's property interest in both computer equipment and all of the uses to which that equipment is put, educate employees about appropriate guidelines for computer use, and diminish any expectation of privacy that an employee might otherwise have regarding electronic communications. An effective electronic communications policy should, at a minimum, contain provisions to address the following:

Ownership of Equipment and Messages

A policy should clearly state that all equipment is owned by the company and is to be used primarily for company business. Depending upon the company, an employer may wish also to claim ownership in all messages or communications created through the use of company equipment.

Sample:

> *"Company X's computers, computer files, the E-mail system, Internet access, and the software furnished to employees are Company property and are to be used primarily for Company business."*

Use of System (Business and/or Personal)

Employees should be told whether company computers are to be used for business purposes only, or whether they may engage in incidental personal use. If the latter, the policy should also set forth any clear limitations the employer wishes to make upon personal use (ex., restricted to non-work hours, restricted to a certain number of hours per month).

Sample:

> *"Incidental and occasional personal use is permitted within reasonable limits, so long as it occurs during non-working hours, does not interfere with the employee's work or the Company's operations, and it complies with the restrictions in this Policy and other Company policies."*

Restrictions on Content

The policy should also set forth any express limitations on message content that the employer wishes to impose (ex., no creation or distribution of chain letters; no solicitations or advertisements for non-company purposes; no searching for other employment). It is particularly important that the policy expressly prohibit use of company computers to create or transmit harassing or defamatory materials or materials that are sexually explicit.

Sample:

> *"Employees may not upload, download, or otherwise transmit via Company X's electronic resources, any material that a reasonable person would consider to be defamatory, offensive, harassing, disruptive, or derogatory. This includes but is not limited to explicit sexual content or images, racial or ethnic slurs, and comments or images that would offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability."*

Prohibited Activities

Employees should be informed of any restrictions on use the employer wishes to impose (ex., no uploading or downloading of confidential or proprietary materials; no using the company's equipment to gain unauthorized access to remote computers or other systems; no use of company computers to access or obtain pornographic or offensive materials; no use of company computers to engage in gambling).

Sample:

> *Employees may not:*
>
> *1. Upload, download, or otherwise transmit without Company authorization copyrighted, trademarked, patented, trade secret, or other confidential, private, or proprietary materials, whether the property of Company X or other companies.*
>
> *2. [Insert any other activities the employer wishes to expressly forbid]*

Security

Employees should be told that they may not engage in activities that could jeopardize the security of the employer's computer systems (ex., disclosing his or her password to others, using or disclosing anyone else's system password, enabling unauthorized persons to access the company's computer systems).

Sample:

> *"Employees will be given an E-Mail account, which may be accessed only through a Company X-assigned username and password. Employees are prohibited from allowing others to send electronic mail from their account and may not use another's account to send their electronic mail. Employees shall not enable unauthorized third parties to access or use Company X's electronic communications systems or otherwise jeopardize the security of the Company's electronic communications systems in any way."*

Employer's Right to Monitor

The policy should expressly reserve to the employer the right to monitor any and all employee use of the company's computer systems. The policy should also remind employees that they have no expectation of privacy in any personal or work messages that they may create or receive using company computer systems.

Sample:

> *"Employees should not assume that any communication, whether business-related or personal, is strictly confidential. Although you will be given a username and password, your electronic communications may still be monitored and/or disclosed consistent with the terms of this Policy.*

Company X has the right, at any time and without prior notice, to monitor, access, retrieve, read, and disclose all information and material—whether business-related or personal—that is created, sent, received, accessed, or stored on its electronic resources."

Notice to employees is important for two reasons. First, it minimizes any expectation of privacy that an employee might otherwise have with regard to e-mail communications or Internet use. Second, under a recent Sixth Circuit case, *Adams v Battle Creek*, 250 F3d 980 (CA 6, 2001), actual notice is a required element of the "business use" exception to the federal Electronic Communications Privacy Act, 18 USC 2510 et seq. (1996).[1]

Consequences of Violating Policy

Employees should be informed that violation of the policy could result in disciplinary action, up to and including discharge. They should also be made aware that they may be held personally responsible for their actions on the Internet.

Sample:

"Violations of this policy, including breaches of confidentiality or security, may result in suspension of e-mail or Internet privileges or other disciplinary action up to and including termination. Company X reserves the right to hold an employee personally liable for any violations of this policy."

Acceptance and Consent to Monitoring

Each employee should be required to sign the policy, acknowledging that he or she had read the policy, agrees to abide by its terms, and consents to any and all company monitoring consistent with the policy."

Sample:

"I have read and fully understand this Policy. I understand that my use of Company X's electronic resources constitutes full acceptance of the terms of this Policy and that, by using Company X's electronic resources, I consent to any and all Company monitoring of that use consistent with this Policy."

As with a notice provision, set forth above, a consent provision accomplishes dual objectives of minimizing employee privacy expectations and providing the employer an exception to the ECPA's bans on interception of electronic communications. 18 USC 2511(2)(d).

"Employees should be informed that violation of the policy could result in disciplinary action, up to and including discharge."

Like any employment policy, an Electronic Communications Policy must be uniformly distributed to all employees to whom it applies. It is also a good idea to remind employees of the existence and terms of the policy on a regular basis.

A Word About Employee Monitoring

The increase in workplace computer use has caused the growth of a new industry focused on preventing abuse. Internet filtering software allows employers to monitor where employees go on the Internet and how much time they spend there. Some software programs permit an employer to set aside periods, such as the lunch hour or after hours, for personal surfing. Others prevent employees from accessing objectionable sites such as gambling or pornography sites. Employers can also purchase software that will enable them to automatically record, filter, and sort every word and every keystroke that an employee types in the creation of e-mail messages. The possibilities are many. The difficult task is finding a program that is right for the size and nature of your or your client's workforce.

The concept of employee monitoring raises privacy issues as well. Employees object to monitoring as an invasion of their privacy. Employers, on the other hand, argue that the debate is one about abuse of company assets. As with many such debates, the risks are high for both sides. The nature and degree of computer monitoring that a company adopts can have a tremendous impact on employee morale. While plaintiffs have begun to challenge the employer's right to monitor or review e-mail and Internet usage, courts have generally ruled that such monitoring is permissible—so long as the employer has a written electronic communications policy that warns the employee. ✦

Andrea J. Bernard is a partner in the Grand Rapids office of Warner Norcross & Judd LLP. She focuses her practice in the area of employment defense and general commercial litigation. She may be reached directly at 616.752.2199 or abernard@wnj.com.

Footnote

1. Under *Adams*, for the "business use" exception to apply, an employer must show that monitoring of employee electronic communications is (1) over equipment supplied by the employer, (2) for a legitimate business purpose; (3) routine; and (4) done with actual notice to the employee. *Adams*, 250 F3d at 984.