LIKE E-MAIL, ONLY FASTER

Don't Forget to Address Instant Messaging in Electronic Communications Policies

JASON KRAUSE

CORPORATE CLIENTS MAY HAVE policies to address Internet activities like e-mailing and downloading, but that's not enough, says Denver lawyer Monique Tuttle. A completely effective policy, she advises, must cover instant messaging—fast becoming a headache for employers.

Instant messaging works like e-mail but is even faster. Information is exchanged at real-time speeds because of software that uses minimal bandwidth and lacks add-ons like storage capacity. Yet the potential for employer liability remains, Tuttle says.

Many corporate clients are unaware that instant messaging is going on at their offices, says Nancy Flynn, executive director of the ePolicy Institute in Columbus, Ohio. With new clients, Flynn's first order of business is to conduct a sweep of the corporate computer system. The results, she says, never fail to surprise: Generally, 50 percent or more of employees turn out to be using instant messaging or other software to communicate with co-workers, business associates, friends and relatives.

"There's a real technology disconnect between what senior management thinks employees are doing," Flynn says, "and what employees ... are really doing."

CUSTOMIZING POLICY CONTENT

GETTING A POLICY FOR ELECTRONIC COMMUNICATIONS IS not difficult. The Electronic Communications Compliance Council, a nonprofit educational group studying electronic communications issues, has a policy available for free download on its Web site (www.TE3C.org) through June. Customizing a policy to protect a specific company, however, requires a bit more effort.

Tuttle says an electronic communications policy could be written broadly enough to include emerging technologies. But she says it is safer to be as specific as possible, and simply update as needed.

When it comes to the nuts and bolts of the policy, companies should decide the level of network security to apply to communications, including access controls like passwords and encryption. They also should decide how much they want to monitor their employees' communications and what sort of penalties they want for abuses.

These decisions shouldn't be made in a vacuum, says Priscilla Emery, chairwoman of the Electronic Communications Compliance Council. "The IT department, legal, records management, compliance and human resources all need to be involved to decide what's permissible."

Records retention is a crucial part of any policy. If a company allows instant messaging, which deletes messages as soon as a computer is turned off, it may need to use business-class instant-messaging software that can archive the messages. Otherwise, a company has no record if something said in an instant message winds up in court. Microsoft and Yahoo sell business versions of their instant-messaging software, which includes security and archiving abilities not found in consumer versions.

Once a new policy is in place, employers must make sure employees realize it's there. A simple notice to that effect, it seems, is not enough. According to a 2004 Massachusetts district court opinion, sending an e-mail notification to employees is inadequate because there's no way to know whether the employee actually read the e-mail or the policy. A better practice, said the court, was to require employees to acknowledge they had read the message, either by clicking on a link or signing a document to that effect. *Campbell v. General Dynamics Government Systems Corp.*, 321 F. Supp. 2d 142.

But experts agree that having a policy is pointless unless it's enforced. "Typically, what we're seeing is that firms don't have a policy in place, and even if they do, it's not enforced," says Paul Chen of Fortiva, an electronic media archiving company in Greenwich, Conn. "If you don't enforce a policy, it's as good as not having one at all." ■

Reprinted with permission *ABA JOURNAL*, May 2005