ON EMPLOYMENT

# Privacy in the workplace

## *Employer/employee rights in the electronic age*

A company's top salesperson's productivity is dwindling. His door is closed more often than it used to be. The company has heard rumors that he is looking at inappropriate Web sites, visiting chat rooms, exchanging inappropriate jokes with his friends outside the office, and looking for a new job online. The company would like to investigate these matters but is not sure what right it has to look at an employee's private affairs. Is the employer entitled to unfettered access to the salesman's computer information?

**By James R. Hammerschmidt**

While there are a multitude of areas where privacy rights intersect employment decisions, a common and complicated issue facing employers today is privacy rights in the evolving electronic workplace.

Such issues often arise in the context of trying to control the electronic workplace. It is possible for a disgruntled employee (or soon-to-be ex-employee) to pirate significant confidential company information, trade secrets or other intellectual property by transferring it to an off-site location or downloading it to a small disc, which he or she puts in a coat pocket on the way out the door. Additionally, e-mail, which is more often than not the preferred means of communication in many companies, forever memorializes potentially damaging information and "discussions," which likely would only have been communicated orally in the "old days."

Privacy issues also arise when employers use technology to evaluate employee performance, monitor quality assurance or investigate employee misconduct. Recent statistics show that nearly 47 percent of large U.S. employers review e-mail messages, 63 percent monitor Internet connections, nearly 10 percent have received subpoenas for e-mail records and approximately the same percentage have defended discrimination or harassment claims founded in part on employee e-mail or Internet use.

*James Hammerschmidt is a principal and member of the Litigation and Employment Law Practice Groups at the law firm of Paley, Rothman, Goldstein, Rosenberg, Eig & Cooper, Chartered in Bethesda. He can be reached at (301) 951-9338 or jrh@paleyrothman.com.*

### Common law rights

An employer must respect common-law privacy rights, which protect employees from unreasonable intrusion. Searching an employee's computer files is today's equivalent of searching an employee's locker or desk.

In deciding whether an intrusion invades a private matter, courts require that an employee have an expectation of privacy and that the expectation be objectively reasonable. Companies must clearly communicate to their employees that computer passwords, phone codes and other such electronic security measures do *not* give employees a right to privacy.

When conducting an investigation or search, a company must go only as far as necessary to fulfill its legitimate business objective. During a harassment investigation, for example, the employer should not read unrelated personal communications or share the alleged harasser's personal communications with persons who do not need to know.

### ECPA

Employers must also be aware of the Electronic Communication Privacy Act of 1986 ("ECPA"). The ECPA prohibits intentional interception, use and disclosure of electronic communications, and also prohibits unauthorized access of stored communications.

Employers who violate the ECPA are subject to both criminal liability, including imprisonment and significant fines, and civil liability, including damages, attorney's fees and litigation costs.

The ECPA does not, however, establish broad workplace privacy rights. Exceptions in the law permit an employer to lawfully monitor its employees' electronic communications, including reviewing e-mail and Internet activity.

First, an employer may monitor employee communications if it has the employee's consent. Consent may be express or implied. The best way to procure such consent is through a written monitoring policy and a signed consent form at the onset of employment.

Second, it is not unlawful for an employer to intercept electronic communications readily accessible to the general public. Employees can have no expectation of privacy in, and no recourse against the company's interception of, electronic bulletin board or chat room conversations.

Third, under the "business purpose exception," an employer may monitor electronic communications for legitimate business purposes. For example, an employer might monitor communication for training or instruction or to ensure customer service. Unlimited monitoring is not justified, however. Monitoring must be narrowly tailored to the company's actual, legitimate business purposes.

The ECPA also allows "providers" of electronic or wire communication services to intercept, disclose or use such communications in the normal course of business when doing so is a necessary incident to the business or to the protection of the provider's rights or property. An employer's internal e-mail system would likely fall within this exception. Protecting against breaches of confidentiality and trade secret theft, conducting system maintenance and investigating harassment claims are probably the best and most common justifications for interceptions.

### Steps to take

An employer should take several important steps to better position itself in the battle for superior rights in the electronic workplace and protect itself from invasion of privacy claims. These steps include:

- Obtaining a written waiver at the commencement of employment;
- Having a written e-mail and computer information policy in the employee handbook that negates any expectation of privacy and notifies employees that e-mail messages, electronic documents, and computer passwords belong to the company, not the employee, and may be monitored;
- Providing guidelines for proper use of the Internet;
- Incorporating provisions concerning the proper use of the Internet, e-mail and electronic communication into the company anti-harassment policy; and
- Limiting access to personal communications to those persons who have a legitimate need to know.

In any case, wholesale monitoring of electronic communications should be avoided. Employers need to take care with both regular monitoring programs for training or other purposes and individualized monitoring where possible employee misconduct is the trigger. It is paramount that employers understand the law before acting and in order to protect their interests in the electronic workplace.