



Keep an Eye on Your Employees... Legally

New communication technology offers employers better ways to monitor employees, but it must be performed within legal limits!

Inherent in the employer-employee relationship is the understanding that the employer should supervise an employee's work activities. Effective supervision ensures that the necessary work is being performed at the time it's needed, resulting in an efficient and profitable operation for the employer. Also, a minority of workers, if left unsupervised, may do or say things that can hurt a business' reputation, reveal trade secrets, or even incur legal liability. While this has always been true to some extent, the rapid changes in communications technology over the past two decades have heightened concerns about it. An employee can hurt a business by saying something inappropriate on the phone, sending an offensive email, visiting web sites that are inappropriate for work, or in a variety of other ways. As a result, employers are using new technology tools to monitor their employees' activities.

Some employers frequently monitor employees' phone conversations. Federal and state law generally allows this for quality control purposes when an employee is on the phone with a client. While some states require advance notification of monitoring to the parties to a call, federal law allows monitoring of business calls with no prior notice. A federal court decision does require employers to stop listening when it becomes apparent that a call is personal in nature, but an employer might monitor all calls made from phones designated as "business use only." It is also legal for employers to obtain lists showing phone numbers dialed from a particular extension and the duration of each call. While the law does not require notifying employees in advance, employers may wish to do so to head off problems.

Courts have also recognized an employer's right to monitor use of its email system. A federal court held that a private sector employee did not have a reasonable expectation of privacy in email messages where he described management in profane and derogatory language. Another court ruled against a CIA employee who violated agency Internet use policy by downloading pornographic material. The federal Electronic Communications Privacy Act of 1986 permits employers to monitor employee email in the ordinary course of business, when the employee consents to monitoring, or when messages are stored on a computer located on an in-house network. Employers may even monitor an employee's keystrokes on a computer to see what and how much text the employee is producing.

Oregon-based law firm DuVal Business Law recommends that employers take the following steps to avoid legal problems arising out of email monitoring:

- Working with legal counsel, develop a comprehensive email and Internet use policy for employees.
- The policy should make it clear that employee communications over the employer's network are not private and that the employer will monitor them for legitimate business reasons.
- The policy should state the workplace rules for Internet use, including types of sites employees may not visit and types of files they may not download. It should also state the penalties for breaking the rules.
- Finally, the policy should state how long the employer will store electronic files and how it will delete them.

DuVal also recommends either having employees sign a copy of the policy before they may receive access to the system or posting the rules on the login screen they see at the start of each day.

Even with these precautions, employee lawsuits for invasion of privacy are still possible. Employers should consider buying employment practices liability insurance to cover them for the cost of defending these suits and the cost of any court-ordered judgments. With this coverage and common sense policies in place, employers can take advantage of Internet technology while not placing themselves at undue risk.