

Privacy in the workplace

Employees, even those who are suspected of fraud or theft, do not relinquish all privacy rights in the workplace. Employers seeking to avoid company losses and expose fraudulent employee conduct may not necessarily justify an expansive search into the employee's personal affairs and effects. The Fourth Amendment of the U.S. Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." Article I, Section 6 of the Illinois Constitution is directly analogous to the federal Constitution. In addition, employees in Illinois are protected under common law from intrusions into seclusion.

Accordingly, these recognized privacy rights must be considered whenever you consider searching what could be considered a "private" employee area. In such situations, an employee may claim that the employer violated a reasonable expectation of privacy. In many cases, whether or not an expectation of privacy is reasonable will depend on what the employer said or did not say to create the expectation of privacy.

It is important for employers to be able to conduct investigations when circumstances give rise to a suspicion of theft or fraud. During such an investigation, an employer should attempt to ensure that employee privacy rights are protected to the extent possible. When appropriate, the employer should consider obtaining the written permission of the employee. However, no workplace investigation, however carefully conducted, will be entirely immune to claims that employee privacy rights were violated.

Recording or monitoring employees

The Federal Wiretap Act generally prohibits the interception, disclosure or intentional use of wire, oral or electronic communications, including those that occur in the workplace.

- A "**wire communication**" is one that carries a person's oral communication over a wire, such as a phone call and includes the "electronic storage of such communication."

- An “**oral communication**” occurs when the individual uttering the communication expected it would be a private conversation.
- An “**electronic communication**” is the transfer of information (writing, images, signals, sounds, data, etc.) transmitted by electronic means including radio waves but is not an oral or wire communication. E-mail, pagers, and cell phone usage are examples of “electronic communications.” “Interception” is the aural or other acquisition of the contents of any oral, wire, or electronic communication, through the use of any electronic or mechanical device.

For example, intercepting a call with a tape recorder connected to a switchboard without an employee’s knowledge is a violation of the Act. However, merely listening to an allegedly illegally-obtained audiotape of private telephone conversations is not a violation of the Act.

The Act provides three defenses for employers.

1. The Act has an exception for employers who act in the “ordinary course of business.” This exception allows an employer to electronically monitor, using a telephone extension, any business-related communication without the employee’s knowledge or consent. An employer may not, however, monitor communications of a purely personal nature. An employer does not violate the Act if it terminates electronic monitoring immediately upon discovering that the monitored call is purely personal.
2. The Act also does not apply if the employer has the consent of one party to the communication, unless the communication is intercepted for the purpose of committing a criminal or tortuous act. Consent may be either express or implied.
3. Under the “provider” exemption, telephone companies and other employers that provide wire communication services may monitor calls for service checks.

The Act provides a civil cause of action to anyone whose communications are unlawfully intercepted. Successful plaintiffs may recover actual or statutory damages (\$10,000 or \$100 a day for each day of violation, whichever is greater), punitive damages, and attorneys’ fees. The Act also makes the unlawful interception, or the attempted interception, of an oral, wire, or electronic communication a felony punishable by fine and/or imprisonment.

The Illinois Eavesdropping Statute

The most significant Illinois statute governing illegal interception of communications is the Illinois Eavesdropping Statute. Use of any eavesdropping device is illegal under the Illinois law. An “eavesdropping device” is “any device capable of being used to hear or

record oral conversation or intercept, retain, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means.” Disclosure of any information which an individual “knows or reasonably should know was obtained through the use of an eavesdropping device” is also illegal.

There are two notable exceptions.

1. Business use

An employer may employ an eavesdropping device for “business use,” including “marketing or opinion research” or “telephone solicitation” for the purpose of “service quality control, education or training of employees,” or “internal research related to marketing or opinion research or telephone solicitation.” One party to the marketing, opinion research or telephone solicitation conversation being monitored must consent to the monitoring. Any recordings may be not be furnished to any law enforcement agency or used in any administrative, judicial or other proceedings, or divulged to any other person. The employer must cease listening and destroy any recording that is not directly related to the business purpose. This exception is quite narrow in application and should not be pursued before discussing with legal counsel.

Employees and applicants for employment must also be informed in writing that they may be monitored as part of their employment. The law also requires that the employer post this information in a prominent place in the workplace. Employers must further provide personal-use telephone lines.

2. Consent

Unlike under federal law, both parties must consent under Illinois law.

Successful plaintiffs may seek punitive damages, actual damages, and injunctive relief. Criminal violations are punishable by up to five years imprisonment.

Searches

An employer should not search federal delivery mail addressed to the employee before it has been delivered. Federal law prohibits any person from taking a letter, postcard or package from the mail. Also, as a general rule, employers should not read correspondence addressed to employees that are marked “personal” or “confidential.”

Employers may search company-owned work areas, lockers, vehicles and other personal items if they have a reasonable basis for doing so. Employers are advised to have a policy authorizing and regulating searches. Employers should proceed with caution if the search requires opening a lock.

Electronic and voice mail

Employees generally have no reasonable expectation of privacy in their electronic mail or voice mail messages, as long as this is communicated and clearly acknowledged via a clear policy restricting employee use of such systems to business use and informing employees that such communications are subject to monitoring. You should notify all employees on a regular basis that their personal use of company equipment is subject to monitoring.

Obtaining employee consent to monitoring your electronic systems is important, as employers can be potentially liable for offensive materials which are easily transmitted among the company via electronic or voice mail. Further, in connection with employee misconduct or other similar matters, reviewing employer communications may provide useful information.

Additionally, you may have a legitimate business need to prevent trade secrets or other confidential information from being transmitted outside the company. See Chapter 37, Changing technology in the workplace.