

6.4: Privacy in the Workplace

Learning Objectives

By the end of this section, you will be able to:

- Explain what constitutes a reasonable right to privacy on the job
- Identify management's responsibilities when monitoring employee behavior at work

Employers are justifiably concerned about threats to and in the workplace, such as theft of property, breaches of data security, identity theft, viewing of pornography, inappropriate and/or offensive behavior, violence, drug use, and others. They seek to minimize these risks, and that often requires monitoring employees at work. Employers might also be concerned about the productivity loss resulting from employees using office technology for personal matters while on the job. At the same time, however, organizations must balance the valid business interests of the company with employees' reasonable expectations of privacy.

Magnifying ethical and legal questions in the area of privacy is the availability of new technology that lets employers track all employee Internet, e-mail, social media, and telephone use. What kind and extent of monitoring do you believe should be allowed? What basic rights to privacy ought a person have at work? Does your view align more closely with the employer's or the employee's?

Legal and Ethical Aspects of Electronic Monitoring

Monitored workstations, cameras, microphones, and other electronic monitoring devices permit employers to oversee virtually every aspect of employees' at-work behavior (Figure 6.14). Technology also allows employers to monitor every aspect of computer use by employees, such as downloads of software and documents, Internet use, images displayed, time a computer has been idle, number of keystrokes per hour, words typed, and the content of e-mails. According to a survey by the American Management Association, 48 percent of employers used a form of video monitoring in the workplace, and 67 percent monitored employee Internet use. In 30 percent of the organizations responding to the survey, this electronic monitoring had ultimately led to an employee's termination.⁴⁹

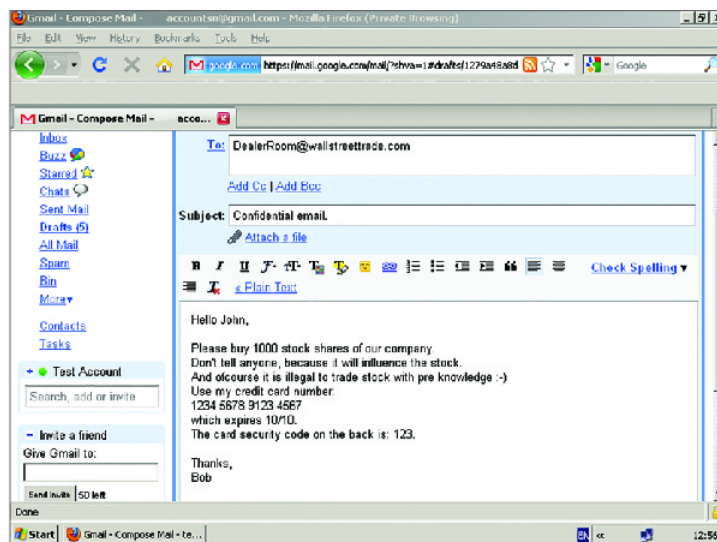


Figure 6.4.14: Electronic monitoring often captures data from cameras, computers, and listening devices. This information can then be used against employees accused of violating company policy, raising privacy concerns. (credit left: modification of "Surveillance video cameras, Gdynia" by Paweł Zdziarski/Wikimedia Commons, CC 2.5; credit right: credit: modification of "Keylogger-screen-capture-example" by "FlippyFlink"/Wikimedia Commons, Public Domain)

The laws and regulations governing electronic monitoring are somewhat indirect and inconsistent. Very few specific federal statutes directly regulate private employers when it comes to broad workplace privacy issues. However, monitoring is subject to various state rules under both statutory and common law, and sometimes federal and state constitutional provisions as well. The

two primary areas of the law related to workplace monitoring are a federal statute called the Electronic Communications Privacy Act of 1986 (ECPA) and various state common law protections against invasion of privacy.⁵⁰

Although the ECPA may appear to prohibit an employer from monitoring its employees' oral, wire, and electronic communications, it contains two big exceptions that weaken its protection of employees' rights. One is the **business purpose exception**. This allows employers—on the basis of legitimate business purposes—to monitor electronic and oral communications, and employers generally assert a legitimate business purpose to be present. The other widely used exception is the **consent exception**, which allows employers to monitor employee communications provided employees have given their consent. According to the Society for Human Resource Management, the ECPA definition of electronic communication applies to the electronic transmission of communications but not to their electronic storage. Therefore, courts have distinguished between monitoring electronic communications such as e-mail during transmission and viewing e-mails in storage. Viewing emails during transmission is broadly allowed, whereas viewing stored e-mail is considered similar to searching an employee's private papers and thus is not routinely allowed under the ECPA unless certain circumstances apply (e.g., the e-mails are stored in the employer's computer systems).⁵¹

In general, it is legal for a company to monitor the use of its own property, including but not limited to computers, laptops, and cell phones. According to the ECPA, an employer-provided computer system is the property of the employer, and when the employer provides employees with a laptop they can take home, it likely violates no laws when it monitors everything employees do with that computer, whether business-related or personal. The same is true of an employer-provided cell phone or tablet, and always true when an employer gives employees notice of a written policy regarding electronic monitoring of equipment supplied by the company. Generally, the same is *not* true of equipment owned by the employee, such as a personal cell phone.

However, an important distinction is based on the issue of consent. The consent provision in the ECPA is not limited to business communications only; therefore, a company might be able to assert the right to monitor personal electronic communications if it can show employee consent (although this is very likely to worry employees, as discussed in the next section). Another consideration is whose e-mail server is being used. The ECPA and some state laws generally make it illegal for employers to intercept private e-mail by using an employee's personal log-on/user ID/password information.

Although the ECPA and National Labor Relations Act are both federal laws, individual states are free to pass laws that impose greater limitations, and several states have done so. Some require employers to provide employees advance written notice that specifies the types or methods of monitoring to which they will be subjected. Examples of state laws creating some degree of protection for workers include laws in California and Pennsylvania that require consent of both parties before any conversation can be monitored or recorded.

Employees can bring common law privacy claims to challenge employer monitoring. (Common laws are those based on prior court decisions rather than on legislatively enacted statutes.) To prevail on a common law claim of invasion of privacy, which is a tort, the employee must demonstrate a right to privacy with respect to the information being monitored. Several state constitutions, such as those in Louisiana, Florida, South Carolina, and California, expressly provide citizens a right to privacy, which may protect employees with respect to monitoring of their personal electronic information and personal communication in the workplace.

One additional regulatory consideration applicable to electronic monitoring is whether the company's workforce is unionized. The National Labor Relations Board, the federal labor law agency, has ruled that the video surveillance of any portion of the workplace is a condition of employment subject to collective bargaining and must be agreed to by the union before implementation, so employees have notice. If a workplace is not unionized (the majority are not), then this federal regulation requiring notice does not apply, and as stated previously in this chapter, if there is any protection at all, it would have to be given by state regulation (which is rare in the private [nongovernmental] sector).

What Constitutes a Reasonable Monitoring Policy?

Many employees generally are not familiar with the specific details of the law. They may feel offended by monitoring, especially of their own equipment. Companies must also consider the effect on workplace morale if everyone feels spied upon, and the risk that some high-performing employees may decide to look elsewhere for career opportunities. Employers should develop a clear, specific, and reasonable monitoring policy. The policy should limit monitoring to that which is directly work related. For example, if a company is concerned about productivity and the goal of monitoring is to keep tabs on employee performance, then neither keystroke logging nor screenshot recording is necessary; software designed to show idle time or personal Internet use would be more helpful in identifying wasted time, which is the ultimate goal.

Employers should always remember their business goals when monitoring employees. It is not only a matter of treating employees ethically; it also makes good business sense to ensure that monitoring pertains only to business matters and does not unnecessarily intrude into the privacy of employees. Perhaps most importantly, in the interest of fairness, the monitoring policy must be communicated to the employees. When, if ever, is it acceptable to monitor without notice to the employee and without his or her knowledge?

link to learning

This [notice by the State of Connecticut](#) mandates that all employers inform employees of the kinds of electronic monitoring of their activities and communications that may be undertaken at work, and the responsibilities of an employer. Read the notice and decide whether you think it is a reasonable policy. Would it make sense to the average worker? Do you think it is unfair to either party?

The Connecticut policy in the preceding Link to Learning applies to all employers (i.e., in state and in private sector workplaces). However, many states have policies that apply only to employees who work for the government. State employees hold a special status that conveys certain state constitutional rights with regard to due process, reasonable searches, and related legal doctrines. The same is true for federal government employees and the U.S. Constitution, which means the government has a duty of fairness in employee surveillance. It does not mean, however, that the government cannot monitor its employees at all, as demonstrated by an incident involving a California police officer. In a unanimous decision in *Ontario v. Quon*,⁵² the U.S. Supreme Court in 2010 ruled in favor of a police chief in Ontario, California, who read nearly five hundred text messages sent by one of his sergeants on a police-issued pager. Many of the text messages were personal and some were sexually explicit. Only a few dozen were work related. The justices agreed that constitutional limits on unreasonable searches by public employers (under the Fourth Amendment) were minimal given a work-related purpose.

This decision creates precedent for more than 25 million employees of federal, state, and local governments and limits their expectation of privacy when using employer-issued tools. “Because the search [by the police chief] was motivated by a legitimate work-related purpose and because it was not excessive in scope, the search was reasonable,” said Justice Anthony M. Kennedy.

In the private sector, where employees are not working for the government and the constitutional prohibition on unreasonable searches and seizures has very little applicability, if any, employers have even more latitude in terms of employee monitoring than in a government setting. The *Ontario v. Quon* case in all likelihood would never even make it to court if the employer were a private-sector company, because the issue of whether getting the text message was a reasonable search and seizure under the Fourth Amendment does not apply in a nongovernment employment setting. The Constitution acts to limit government intrusions but does not generally restrict private companies in this type of situation. However, ethical considerations may encourage private-sector employers to treat their workers respectfully, even if not required by law.

WHAT WOULD YOU DO?

Security versus Privacy

You manage a large, high-end jewelry store with an international clientele. Your workforce of 150 is demographically diverse, and your employees are trustworthy as a rule. However, you have experienced some unexplained loss of inventory and suspect a couple of employees are stealing valuable pieces, removing them from backroom storage safes and handing them off to another person somewhere in the store who leaves with them or to a third person pretending to be a customer. To prevent this, your assistant managers are urging you to place discreet cameras in the restrooms and break rooms, where these exchanges are likely occurring. Some managers might be concerned about using cameras at all due to privacy issues; others might want to use them without notifying employees or putting up signs because they do not want to tip off the suspects or deal with the negative reaction of the workforce (although that brings up invasion of privacy issues). You are weighing the pros of catching the thieves against the possible loss of other employees’ trust.

Critical Thinking

- What issues must you confront as you decide whether you will take the recommendation of your assistant managers?
- What, ultimately, will you do? Explain your decision.

Drug Testing in the Workplace

Key issues that arise about a drug testing or monitoring program begin with whether an employer wants or needs to do it. Is it required by law for a particular job, under state or local regulations? Is it for pre-employment clearance? Does the employer need employees' permission? Does a failed test require mandatory termination? With the exception of employers in industries regulated by the federal government, such as airlines, trucking companies, rail lines, and national security-related firms, federal law is not controlling on the issue of drug testing in the workplace; it is largely a state issue. At the federal level, the Department of Transportation does mandate drug testing for workers such as airline crews and railway conductors and has a specific procedure that must be followed. However, for the most part, drug testing is not mandatory and depends on whether the employer wants to do it. Multiple states do regulate drug testing, but to varying degrees, and there is no common standard to be followed.

Testing of job applicants is the most common form of drug testing. State laws typically allow it, but the employer must follow state rules, if they exist, about providing notice and following standard procedures intended to prevent inaccurate samples. Testing current employees is much less common, primarily due to cost; however, companies that do use drug testing include some in the pharmaceutical and financial services industries. Some states put legal constraints on drug testing of private-sector employees. For example, in a few states, the job must include the possibility of property damage or injury to others, or the employer must believe the employee is using drugs.

Challenging a drug test is difficult because tests are considered highly accurate. An applicant or employee can refuse to take the test, but that often means not being hired or losing the job, assuming the worker is an employee at will. The concept of **employment at will** affirms that either the employee or the employer may dissolve an employment arrangement at will (i.e., without cause and at any time unless an employment contract is in effect that stipulates differently). Most workers are considered employees at will because neither the employer nor employee is obligated to the other; the worker can quit or be fired at any time for any reason because there is no contractual obligation. In some states, the employee risks not only job loss but also the denial of unemployment benefits if fired for refusing to take a drug test. Thus, the key concept that makes drug testing possible is employment at will, which covers approximately 85 percent of the employees in the private sector (unionized workers and top executives have contracts and thus are not at will, nor are government employees who have due process rights). The only legal limitation is that, in some states, the drug testing procedure must be fair, accurate, and designed to minimize errors and false-positive results.

The drug testing process, however, raises some difficult privacy issues. Employers want and are allowed to protect against specimen tampering by taking such steps as requiring subjects to wear a hospital gown. Some employers use test monitors who check the temperature of the urine and/or listen as a urine sample is collected. According to the Cornell University Law School Legal Information Institute, some state courts (e.g., Georgia, Louisiana, Hawaii) have found it an unreasonable invasion of privacy for the monitor to watch an employee in the restroom; however, in other states (e.g., Texas, Nevada), this is allowed.⁵³

Case examples abound of challenges based on privacy concerns. In an article in the *Harvard Journal of Law and Technology*, University of Houston Law School professor Mark Rothstein, who is director of the Health Law and Policy Institute, summarized examples of legal challenges.⁵⁴ In one case, the court ruled that an employer engaged in unlawful retaliation as defined by the Mine Safety and Health Act. The employer dismissed two employees who were required to urinate in the presence of others but found themselves unable to do so. In a different case, \$125,000 in tort damages was awarded to a worker for invasion of privacy and negligent infliction of emotional distress as a consequence of his being forced to submit a urine sample as he was being directly observed.

This page titled [6.4: Privacy in the Workplace](#) is shared under a [CC BY 4.0](#) license and was authored, remixed, and/or curated by [OpenStax](#) via [source content](#) that was edited to the style and standards of the LibreTexts platform.