Workplace Privacy and Employee Monitoring

Posted: Mar 01 1993 | Revised: Mar 25 2019

This publication is for historical purposes only. Visit this article for updated information.

1. Introduction

A majority of employers monitor their employees. The Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute shows the pervasiveness of employee monitoring. Employers are motivated by concern over litigation and the increasing role that electronic evidence plays in lawsuits and government agency investigations. Such monitoring is virtually unregulated. Therefore, unless company policy specifically states otherwise (and even this is not assured), your employer may monitor most of your workplace activity. These policies may be communicated through employee handbooks, by memos, in union contracts, and by other means. Courts often have found that when employees are on the job, their expectation of privacy is limited.

2. Computers and Workstations

Employers generally are allowed to monitor your activity on a workplace computer or workstation. Since the employer owns the computer network and the terminals, he or she is free to use them to monitor employees. Technology exists for your employer to monitor almost any aspect of your computer or workstation use. There are several types of monitoring:

- Computer software can enable employers to see what is on the screen or stored in the employees' computer terminals and hard disks.
- Employers can keep track of the amount of time an employee spends away from the computer or idle time at the terminal.

- Keystroke monitoring tell an employer how many keystrokes per hour each employee is performing.

Employees are given some protection from computer and other forms of electronic monitoring under certain circumstances. Union contracts, for example, may limit the employer's right to monitor. Also, public sector employees may have some minimal rights under the United States Constitution, in particular the Fourth Amendment which safeguards against unreasonable search and seizure. Additional statutory rights for employees in **California** are explained in *Privacy Rights of Employees Using Workplace Computers in California*.

Most computer monitoring equipment allows employers to monitor without the employees' knowledge. However, some employers do notify employees that monitoring takes place. This information may be communicated in memos, employee handbooks, union contracts, at meetings or on a sticker attached to the computer.

3. Email and Instant Messaging

If an email or instant messaging system is used at a company, the employer owns it and is allowed to review its contents. Messages sent within the company as well as those that are sent or received to or from another person or company can be subject to monitoring by your employer. Employees should assume that their email and instant messaging on a company system is being monitored and is not private. Several workplace privacy court cases have been decided in the employer's favor. See for example:

- Smyth v. Pillsbury
- Falmouth Firefighters Union v. Town of Falmouth

Some employers use encryption to protect the privacy of their employees' email. Encryption involves scrambling the message at the sender's terminal, then unscrambling the message at the terminal of the receiver. This ensures the message is read only by the sender and his or her intended recipient. While this system prevents coworkers and hackers from reading your email, your employer may still have access to these messages.

4. Telephones

In most instances, employers may listen to your phone calls at work. For example, employers may monitor calls with clients or customers for reasons of quality control. However, when the parties to the call are all in California, state law requires that they be informed that the conversation is recorded or monitored by either putting a beep tone on the line or playing a recorded message. Federal law, which regulates phone calls with persons outside the state, does allow unannounced monitoring for business-related calls. See Electronic Communications Privacy Act, 18 USC 2510, et. seq.

An important exception is made for personal calls. Under federal case law, when an employer realizes the call is personal, he or she must immediately stop monitoring the call. (Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983)). However, when employees are told not to make

personal calls from specified business phones, the employee then takes the risk that calls on those phones may be monitored.

5. Mobile Devices

Generally, your employer may monitor your use of any employer-provided mobile phone or device. Monitoring apps can secretly record your text messages, email, Internet usage, location, contacts, call logs, photos and videos.

Some employers allow employees to use their own personal mobile devices for work purposes, either instead of or in addition to employer-provided devices. This is often referred to as bring your own device (BYOD). BYOD programs pose great challenges in balancing the security of employer data and protecting employee privacy.

BYOD policies may appear in a BYOD agreement, employment contract, orientation materials, employee manual, when an employee decides to use his device, or when the employee installs an employer's mobile device management (MDM) software on his/her own device. It is important for employees to read an employer's BYOD policy before participating in a BYOD program, and to ask questions.

The law concerning employee rights when they use their own devices is emerging as more employees use the same mobile devices for both work and personal purposes. This means legal issues are less likely to have clear cut answers. For a more complete discussion of these issues, see PRC's guide Bring Your Own Device . . . at Your Own Risk.

6. Audio and Video Recording

Video monitoring is a commonly used method for deterring theft, maintaining security and monitoring employees. Federal law does not prevent video monitoring even when the employee does not know or consent to being monitored.

In some instances, courts have upheld employee privacy. Specifically, some courts have sided with employee privacy in instances where the monitoring has been physically invasive, such as hidden cameras in a locker room or bathroom. Some state laws may have restrictions on where, how and why an employer may videotape employees. Labor unions may negotiate limitations on video recordings of unionized workers. Union members should speak with a union representative if they have concerns about workplace video monitoring.

Video cameras that also capture audio recordings may be subject to laws relating to audio recording, including wiretap and eavesdropping laws. Federal law does not prohibit audio recording of phone conversations as long as one party on the call consents to recording. Most states have extended this law to include recording in-person conversations. Some states have laws that require that all parties in a conversation consent to audio recording. For a state-

specific guideline of laws regarding audio recording, visit Can We Tape? A Practical Guide to Taping Phone Calls and In-Person Conversation in the 50 States and D.C.

7. Location (GPS) Tracking

Generally, employers may use Global Positioning Systems (GPS) devices to track employees in employer-owned vehicles. While few courts have addressed GPS tracking, most have held that employers may use GPS tracking devices on company-owned equipment, where the employee does not have a reasonable expectation of privacy. California, Minnesota, Tennessee, and Texas, have laws preventing the use of mobile tracking devices in order to track other individuals. However, these statutes do not apply to installing GPS devices in employer-owned vehicles.

Some employers may use cell phone tracking to monitor employee location.

8. U.S. Postal Mail

Employers generally may open mail addressed to you at your workplace. Although Federal law prohibits mail obstruction, mail is considered delivered when it reaches the workplace. The USPS Domestic Mail Manual (DMM) deals with the handling of mail addressed to an individual at an organization.

The DMM provides:

All mail addressed to a governmental or nongovernmental organization or to an individual by name or title at the address of the organization is delivered to the organization, as is similarly addressed mail for former officials, employees, contractors, agents, etc. If disagreement arises where any such mail should be delivered, it must be delivered under the order of the organization's president or equivalent official.

DMM Chapter 508, Section 1.5.1

Accordingly, an employer does not violate the law by opening an employee's personal mail addressed to the employee at the employer's address. After USPS delivers the mail to your employer, it's up to the organization to decide how to distribute it. For example, a mail room employee might be authorized to open all mail before sorting and delivering it. This includes any mail marked "personal" or "confidential" for a specific employee.

There could be certain limited situations in which opening and reading an employee's mail might be considered an invasion of privacy. These situations would be very fact-specific and guided by common law principles of tort law. Employees should consult an attorney for guidance.

9. Social Media

Many companies have social media policies that limit what you can and cannot post on social networking sites about your employer. Some states have laws that prohibit employers from

disciplining an employee based on off-duty activity on social networking sites, unless the activity can be shown to damage the company in some way. In general, posts that are work-related have the potential to cause the company damage. Anti-discrimination laws prohibit employers from disciplining employees based on age, race, color, religion, national origin or gender.

The National Labor Relations Board (NLRB) has issued a number of rulings involving questions about employer social media policies. The NLRB has indicated that these cases are extremely fact-specific. It has provided the following general guidance:

- Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.
- An employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.

Several states have enacted legislation protecting employees or job applicants from employers that require them to provide a user name or password for a social media account. For a current list of state laws and pending legislation see NCSL's List.

Learn More

Communications
Education
Employment
Financial
Health
Personal
Retail
Security
Technology

Background Checks
Credit Reports
Data Breaches
Data Brokers
Debt Collection
Government IDs
Identity Theft
Spam

Speak Up

Share Your Story

Support Us

Donate