

Fact Sheet 7:

Workplace Privacy and Employee Monitoring

 [Send to Printer](#)

Copyright © 1993 - 2013
Privacy Rights Clearinghouse
Posted March 1993
Revised February 2013

1. [Introduction](#)
2. [Telephone Monitoring](#)
 - [Can my employer listen to my phone calls at work?](#)
 - [If I wear a headset, are my conversations with co-workers subject to monitoring?](#)
 - [Can my employer obtain a record of my phone calls?](#)
3. [Computer Monitoring](#)
 - [Is my employer allowed to see what is on my terminal while I am working?](#)
 - [How can I tell if I am being monitored at my terminal?](#)
4. [Electronic Mail, Voice Mail and Postal Mail](#)
 - [Is electronic mail private? What about voice mail?](#)
 - [When I delete messages from my terminal, are they still in the system?](#)
 - [My employer's electronic mail system has an option for marking messages as "private." Are those messages protected?](#)
 - [Is there ever a circumstance in which my messages are private?](#)
 - [Are my text messages on an employer-provided cell phone private?](#)
 - [Can my employer monitor an employer-provided smartphone?](#)
 - [Can my employer open postal mail addressed to me at my workplace?](#)
5. [Social Media Monitoring](#)
 - [Can I be fired over what I post on social media sites?](#)
6. [Video Monitoring](#)
 - [Can employers use video monitoring in the workplace?](#)
 - [Are there situations where an employer cannot use video cameras?](#)
 - [What about video cameras that include audio surveillance?](#)
7. [Workplace Privacy Protections](#)
 - [What about my employer's promises regarding e-mail and other workplace privacy issues. Are they legally binding?](#)
 - [Can an employer use Global Positioning Systems \(GPS\) to track employees?](#)
 - [Are there any laws that deal with workplace privacy?](#)
 - [Are there organizations that assist employees regarding workplace privacy?](#)
8. [Resources](#)

1. Introduction

Employers want to be sure their employees are doing a good job, but employees don't want their every sneeze or trip to the water cooler logged. That's the essential conflict of workplace monitoring.

New technologies make it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals, through electronic and voice mail, and when employees are using the Internet. Such monitoring is virtually unregulated. Therefore, unless company policy specifically states otherwise (and even this is not assured), your employer may listen, watch and read most of your workplace communications.

One company offers technology that claims to provide insight into individual employee behavior based on the trail of "digital footprints" created each day in the workplace. This behavioral modeling technology can piece together all of these electronic records to provide behavior patterns that employers may utilize to evaluate employee performance and conduct. For example, it might look for word patterns, changes in language or style, and communication patterns between individuals.

Recent surveys have found that a majority of employers monitor their employees. They are motivated by concern over litigation and the increasing role that electronic evidence plays in lawsuits and government agency investigations.

A 2007 survey by the [American Management Association and the ePolicy Institute](#) found that two-thirds of employers monitor their employees' web site visits in order to prevent inappropriate surfing. And 65% use software to block connections to web sites deemed off limits for employees. This is a 27% increase since 2001 when the survey was first conducted. Employers are concerned about employees visiting adult sites with sexual content, as well as games, social networking, entertainment, shopping and auctions, sports, and external blogs. Of the 43% of companies that monitor e-mail, nearly three-fourths use technology to automatically monitor e-mail. And 28% of employers have fired workers for e-mail misuse.

Close to half of employers track content, keystrokes, and time spent at the keyboard. And 12% monitor blogs to see what is being written about the company. Another 10% monitor social networking sites.

Almost half of the companies use video monitoring to counter theft, violence and sabotage. Of those, only 7% state they use video surveillance to track employees' on-the-job performance. Most employers notify employees of anti-theft video surveillance (78%) and performance-related video monitoring (89%).

2. Telephone Monitoring

Can my employer listen to my phone calls at work?

In most instances, yes. 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. (California Public Utilities Commission General Order 107-B, www.cpuc.ca.gov/Published/Graphics/567.pdf)

Not every business is aware of this requirement, so your calls might still be monitored without a warning. 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.

Privacy Tip: The best way to ensure the privacy of your personal calls made at work is to use your own mobile phone, a pay phone, or a separate phone designated by your employer for personal calls.

If I wear a headset, are my conversations with co-workers subject to monitoring?

Yes. The conversations you have with co-workers are subject to monitoring by your employer in the same way that your conversations with clients or customers are. If you wear a headset, you should use the same care you would if you were talking to a customer or client on the phone. Some headsets have "mute" buttons which allow you to turn off the transmitter when you are not using the telephone.

Can my employer obtain a record of my phone calls?

Yes. Telephone numbers dialed from phone extensions can be recorded by a device called a pen register. It allows the employer to see a list of phone numbers dialed by your extension and the length of each call. This information may be used to evaluate the amount of time spent by employees with clients.

Employers often use pen registers to monitor employees with jobs in which telephones are used extensively. Frequently, employees are concerned that the information gathered from the pen register is unfairly used to evaluate their efficiency with clients without consideration of the quality of service.

3. Computer Monitoring

If you have a computer terminal at your job, it may be your employer's window into your workspace. There are several types of computer monitoring.

1. Employers can use computer software that enables them to see what is on the screen or stored in the employees' computer terminals and hard disks. Employers can monitor Internet usage such as web-surfing and electronic mail.

People involved in intensive word-processing and data entry jobs may be subject to

keystroke monitoring. Such systems tell the manager how many keystrokes per hour each employee is performing. It also may inform employees if they are above or below the standard number of keystrokes expected. Keystroke monitoring has been linked with health problems including stress disabilities and physical problems like carpal tunnel syndrome.

2. Another computer monitoring technique allows employers to keep track of the amount of time an employee spends away from the computer or idle time at the terminal.

Is my employer allowed to see what is on my terminal while I am working?

Generally, yes. Since the employer owns the computer network and the terminals, he or she is free to use them to monitor employees. 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.

There may be some additional rights for employees in California given specific statutes of that state. See the paper by Los Angeles attorneys John Caragozian and Donald Warner, Jr., titled "[Privacy Rights of Employees Using Workplace Computers in California](#)," published in 2000.

How can I tell if I am being monitored at my terminal?

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.

In most cases, employees find out about computer monitoring during a performance evaluation when the information collected is used to evaluate the employee's work.

4. Electronic Mail, Voice Mail and Postal Mail

Is electronic mail private? What about voice mail?

In most cases, no. If an electronic mail (e-mail) 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 from your terminal to another company or from another company to you can be subject to monitoring by your employer. This includes web-based email accounts such as Yahoo and Hotmail as well as instant messages. The same holds true for voice mail systems. In general, employees should not assume that these activities are not being monitored and are private. Several workplace privacy court cases have been decided in the employer's favor. See for example:

- Smyth v. Pillsbury, www.loundy.com/CASES/Smyth_v_Pillsbury.html
- Falmouth Firefighters Union v. Town of Falmouth

At least one Court has placed some limitations on an employer's policy that personal emails are not private. On March 30, 2010, the New Jersey Supreme Court ruled that attorneys for an employer violated the privacy rights of a former employee and the rules of professional conduct by reading emails the employee sent to her counsel on a company laptop through her personal password-protected Yahoo email account. [*Stengart v. LovingCare Agency, Inc.*](#), 2010 WL 1189458 (N.J. March 30, 2010).

The Court held that the attorney-client privilege applied to emails even though the employer had a general policy stating that the employee should have no reasonable expectation of privacy in communication sent over company equipment. The court zeroed in on the attorney-client privileged nature of the emails. The court did not address whether the employee would have had a reasonable expectation of privacy with respect to personal email communications with a non-lawyer.

In [*Holmes v. Petrovich Development Company, LLC*](#), a California court ruled that emails sent by an employee to her attorney from a computer in her workplace were not protected by attorney-client privilege. However, unlike the *Stengart* case, this employee used a company email account (rather than a personal webmail account) to send the emails. The court noted that the employee had been (1) told of the company's policy that its computers were to be used only for company business, (2) warned that the company would monitor its computers for compliance with this policy, and (3) advised that employees using company computers have no right of privacy.

When I delete messages from my terminal, are they still in the system?

Yes. Electronic and voice mail systems retain messages in memory even after they have been deleted. Although it appears they are erased, they are often permanently "backed up" on magnetic tape, along with other important data from the computer system.

My employer's electronic mail system has an option for marking messages as "private." Are those messages protected?

In most cases, no. Many electronic mail systems have this option, but it does not guarantee your messages are kept confidential. An exception is when an employer's written electronic mail policy states that messages marked "private" are kept confidential. Even in this situation, however, there may be exceptions. (See *Smyth v. Pillsbury* above.)

Is there ever a circumstance in which my messages are private?

Some employers use encryption to protect the privacy of their employees' electronic mail. 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 co-workers and industrial "spies" from reading your electronic mail, your employer may still have access to the unscrambled messages.

Are my text messages on an employer-provided cell phone private?

In a June 2010 decision, *City of Ontario v. Quon*, the Supreme Court unanimously upheld the search of a police officer's personal messages on a government-owned pager, saying it did not violate his constitutional rights. The warrantless search was not an unreasonable violation of the officer's 4th Amendment rights because it was motivated by legitimate work-related purposes. The city was trying to determine whether it needed to modify its wireless contract, which imposed fees after employees exceeded character limits on text messages.

The city obtained a transcript of Quon's messages during an investigation to determine whether officers were using their pagers for personal messages. The transcripts showed that Quon had been exchanging sexually explicit messages. The Court's decision generally allows government employers to look at workers' electronic messages if employers have reasonable, work-related grounds.

The privacy issue in *City of Ontario v. Quon* involved a government intrusion into personal communications, that is, whether or not the 4th Amendment applied to the electronic communications of public employees. The 4th Amendment would not apply to a private employer. However, the decision could have an impact on future court decisions involving private employers.

There is one important lesson to be had from the Quon case: An employer's policy regarding monitoring need not specify every means of communication subject to the policy. As an employee, you should assume that any electronic device provided by an employer may be subject to monitoring, whether or not such a device is specifically mentioned in a written policy.

Can my employer monitor an employer-provided smartphone?

Under most circumstances, your employer may legally monitor your usage of an employer-provided smartphone. Monitoring apps can secretly record your text messages, email, Web usage, location, contacts, call logs, photos and videos. Read more about these apps at <http://usatoday30.usatoday.com/tech/columnist/kimkomando/story/2012-02-24/work-monitor-smartphone/53221804/1>.

Can my employer open postal mail addressed to me at my workplace?

Generally yes. 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 mailroom 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.

<http://www.businessmanagementdaily.com/19709/mail-policy-considerations-maintaining-the-right-to-open-employee-mail>.

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.

5. Social Media Monitoring

Can I be fired over what I post on social media sites?

It depends on the policies your employer has in place and your State law.

Many companies have social media policies that limit what you can and cannot post on social networking sites about your employer. A website called Compliance Building has a [database of social media policies](#) for hundreds of companies. You should ask your supervisor or human resources department what the policy is for your company.

Some states, including California, Colorado, Connecticut, North Dakota and New York, 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. If you feel that you have been discriminated against, contact a lawyer. You can find a lawyer who specializes in employment law via the [National Employment Lawyers Association](#).

There is no federal law that we are aware of that an employer is breaking by monitoring employees on social networking sites. In fact, employers can even hire third-party companies to monitor online employee activity for them. In March, 2010 a company called Teneros launched a "Social Sentry" service that tracks the online activity of employees across social networking sites. According to an [article by Read Write Web](#) employers use the service to "make sure that employees don't leak sensitive information on social networks or engage in any behavior that could damage a company's reputation."

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.

You can read more about these rulings at <http://ebn.benefitnews.com/news/nlrb-offers-long-awaited-guidance-social-media-policies-2729827-1.html> and http://www.nytimes.com/2013/01/22/technology/employers-social-media-policies-come-under-regulatory-scrutiny.html?_r=0&pagewanted=all&pagewanted=print.

6. Video Monitoring

Can employers use video monitoring in the workplace?

For the most part, yes. Video monitoring is a commonplace method of deterring theft, maintaining security and monitoring employees. For example, a bank may utilize video monitoring to prevent or collect evidence on a robbery. A company may also use video monitoring in a parking garage as a security measure for employee safety.

Employers may also use cameras to monitor employee productivity and prevent internal theft. Currently, federal law does not prevent video monitoring even when the employee does not know or consent to being monitored.

Are there situations where an employer cannot use video cameras?

In some instances, courts have upheld employee privacy. Specifically, 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. See National Workrights Institute's [Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection](#) for a more in-depth discussion.

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.

What about video cameras that include audio surveillance?

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. Twelve 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.](#) (The Reporters Committee for Freedom of the Press).

6. Workplace Privacy Protections

What about my employer's promises regarding email and other workplace privacy issues. Are they legally binding?

Not necessarily. Usually, when an employer states a policy regarding any issue in the workplace, including privacy issues, that policy is legally binding. Policies can be communicated in various ways: through employee handbooks, via memos, and in union contracts. For example, if an employer explicitly states that employees will be notified when telephone monitoring takes place, the employer generally must honor that policy. There are usually exceptions for investigations of wrong-doing. If you are not already aware of your employer's workplace privacy policies, it is a good idea to become informed.

In *Smyth v. Pillsbury* (C.A. NO. 95-5712, U.S. District Court for the Eastern District of Pennsylvania, Jan. 18, 1996, Decided, Jan. 23, 1996), the employee's termination was upheld by the court, even though the company had a policy of allowing e-mail use for personal communications. In this case, the employee had sent messages to co-workers that were deemed highly inappropriate for workplace communications.

Can an employer use Global Positioning Systems (GPS) to track employees?

Generally, employers may use GPS devices to track employees in employer-owned vehicles. Some courts have extended this to employee-owned vehicles as well. The law on this is rapidly evolving. Learn more by reading [GPS in the Workplace](#).

Are there any laws that deal with workplace privacy?

Currently there are very few laws regulating employee monitoring. If you are concerned about this issue, contact your federal legislators, especially the members of the House and Senate Labor committees in Congress.

Are there organizations that assist employees regarding workplace privacy?

Yes. There are several groups that are actively involved in workplace monitoring issues and that advocate stronger government regulation of employee monitoring activities.

- **National Work Rights Institute**

166 Wall St.
Princeton, NJ 08540
[\(609\) 683-0313](tel:6096830313)
Web: www.workrights.org

- **9 to 5, the National Association of Working Women**

207 East Buffalo St., #211
Milwaukee, WI 53202
[\(414\) 274-0925](tel:4142740925)
Hotline [\(800\) 522-0925](tel:8005220925)
Web: www.9to5.org

- **Workplace Fairness**

www.workplacefairness.org
Affiliated with the National Employment Lawyers Association, www.nela.org

- **American Civil Liberties Union**
125 Broad Street, 18th Floor
New York, NY 10004-2400
[\(212\) 549-2500](tel:(212)549-2500)
Publications Ordering: 1-800-775-ACLU (2258)
Web: www.aclu.org

The American Civil Liberties Union (ACLU) also has information related to workplace privacy issues that are not discussed in this fact sheet. Some of the issues of growing concern involve psychological testing, drug testing, polygraph or lie-detector testing and off-the-job surveillance of employees. Visit the ACLU's Web site at www.aclu.org.

7. Resources

- **Workplace Fairness "Surveillance at Work"**
<http://www.workplacefairness.org/surveillance>
- **Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection** <http://workrights.us/?products=electronic-monitoring-in-the-workplace-common-law-federal-statutory-protection>

Tags: [Background Checks & Workplace](#) [Fact Sheet](#) [eavesdropping](#) [employee](#)
[monitoring](#) [employment](#) [telephone](#) [wiretapping](#) [workplace](#)

 [Send to Printer](#)  [Post to Twitter](#)

Copyright © Privacy Rights Clearinghouse. This copyrighted document may be copied and distributed for nonprofit, educational purposes only. For distribution, see our [copyright and reprint guidelines](#). The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse.