Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Workplace Privacy and Employee Monitoring [1]

Posted Mar 01 1993
Revised May 14 2018

1. Introduction

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. Almost everything you do on your office computer can be monitored. 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. Courts often have found that when employees are using an employer's equipment, their expectation of privacy is limited.

Employers use technology to provide insight into employee behavior based on the trail of "digital footprints" created each day in the workplace. This 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. This makes it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals, through email and voice mail, and when employees are online.

It's important to be aware that your employer's promises regarding workplace privacy issues may not always 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.

2. Computer and Workstation Monitoring

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 [2]*.

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 Monitoring

If an email 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. *This may include Internet-based email accounts such as Gmail and Yahoo Mail as well as instant messages.*

Employees should assume that their email 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 [3]
- Falmouth Firefighters Union v. Town of Falmouth [4]

Are emails to an employee's attorney protected by attorney-client privilege?

A New Jersey court has placed some limitations on an employer's policy that personal emails are not private. In *Stengart v. LovingCare Agency, Inc* [5]., the 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.

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* [6]. [7] 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.

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

In most cases, no. Many email systems have this option, but it does not guarantee your messages are kept confidential. An exception is when an employer's written email 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' 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 co-workers and industrial "spies" from reading your email, your employer may still have access to the unscrambled messages.

4. Telephone Monitoring

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 [8], 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. [9], 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

Can my employer monitor my *employer-provided* mobile phone or device?

Under most circumstances, your employer may legally monitor your usage of an employer-provided mobile phone or device. Monitoring apps [10] can secretly record your text messages, email, Internet usage, location, contacts, call logs, photos and videos.

What are my rights if I use *my own* mobile device for work purposes?

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. [11]

What can my employer do with access to my BYOD device?

This would depend upon the BYOD agreement (or other BYOD policy documents) provided by your employer and the specific software being utilized. Potentially, an employer could:

- Lock, disable or wipe the employee's personal device or delete any and all data contained on the phone.
- Access the device
- Access phone records or contacts
- Access to social media or other account username and passwords
- Monitor GPS and location information
- View Internet browsing history
- View pictures, video, or other media
- View personal emails
- View chat and messaging histories

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

In *City of Ontario v. Quon* [12] (2010), 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 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.

6. Audio and 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, 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.

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. 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 [13].

7. 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 [14] 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 [15].

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

8. 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 [16]

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 [17] 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.

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 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 [18] for hundreds of companies. You should ask your supervisor or human resources

department what the policy is for your company.

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.

Can an employer require a job applicant or employee to provide a user name or password for a social media account?

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 [19].

10. Resources

There are several organizations that are actively involved in workplace monitoring issues and that advocate stronger government regulation of employee monitoring activities. Some of these groups can provide assistance to employees having workplace issues:

- **National Work Rights Institute**
  166 Wall St.
  Princeton, NJ 08540
  (609) 683-0313
  Web: www.workrights.org [20]

- **9 to 5, the National Association of Working Women**
  207 East Buffalo St., #211
  Milwaukee, WI 53202
  (414) 274-0925
  Hotline (800) 522-0925
  Web: www.9to5.org [21]

- **Workplace Fairness**
  www.workplacefairness.org
  [22]Affiliated with the National Employment Lawyers Association, www.nela.org [23]

Many **State Agencies** [24] deal with workplace issues. [24]

You can find an **attorney** who specializes in employment law via the National Employment Lawyers Association [25].

The 2007 (most recent available) Electronic Monitoring & Surveillance Survey [26] from American Management Association and The ePolicy Institute shows the pervasiveness of employee monitoring.

Source URL (modified on May 14, 2018): https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring

Links
[1] https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring
[2] https://www.privacyrights.org/ar/employees-rights.htm
[3] http://www.loundy.com/CASES/Smyth_v_Pillsbury.html
[4] http://www.employmentmattersblog.com/2012/05/no-expectation-of-privacy-in-emails-sent-over-employers-email-account-massachusetts-court-decides/

[5] http://caselaw.findlaw.com/nj-supreme-court/1522648.html
[6] http://caselaw.findlaw.com/ca-court-of-appeal/1552780.html
[7] http://www.courtinfo.ca.gov/opinions/documents/C059133.PDF
[8] http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119
[9] http://law.justia.com/cases/federal/appellate-courts/F2/704/577/107387/
[10] http://usatoday30.usatoday.com/tech/columnist/kimkomando/story/2012-02-24/work-monitor-smartphone/53221804/1
[11] https://www.privacyrights.org/bring-your-own-device-risks
[12] http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf
[13] http://www.rcfp.org/reporters-recording-guide
[14] http://www.workplaceprivacyreport.com/2014/09/articles/workplace-privacy/key-considerations-when-monitoring-employees-using-gps-tracking-devices/
[15] http://privacylaw.proskauer.com/2012/04/articles/workplace-privacy/gps-in-the-workplace/
[16] https://pe.usps.com/text/dmm300/508.htm#ep1132464
[17] http://www.businessmanagementdaily.com/19709/mail-policy-considerations-maintaining-the-right-to-open-employee-mail
[18] http://www.compliancebuilding.com/about/publications/social-media-policies/
[19] http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx
[20] http://workrights.us/
[21] http://9to5.org/
[22] http://www.workplacefairness.org/
[23] http://www.nela.org/
[24] http://www.workplacefairness.org/stateagencies
[25] http://exchange.nela.org/network/findalawyer
[26] http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx