

11.3: Workplace Privacy

Employees generally do not have a reasonable expectation of privacy in the workplace, especially when using company equipment or when the employer has a policy stating employees may be monitored. However, some areas such as employee restrooms and locker rooms may not be monitored. Courts have held employees do not give up all expectations of privacy by the nature of their employment. Therefore, employers should ensure that they limit monitoring activities to reasonable places where the employer has a legitimate business interest for doing so.

Hiring Process

Employers often run background checks on prospective employees as part of their hiring process. Depending on what type of background check is done and the information used, a range of privacy issues are involved. Some states regulate the type of documents that a prospective employer may consider when making hiring decisions. Businesses need to ensure they comply with all state laws where they hire employees.

The use of artificial intelligence (AI) is a growing trend in recruiting and hiring. AI is often used to review resumes, applications, and publicly available social media. AI-powered video-interview platforms apply algorithms to video-recorded interviews to facilitate an employer's assessment of applicants.

Illinois was the first state to pass an AI Interview Act, which requires prospective employers to notify applicants of their use of AI and to obtain their consent before using AI tools on their application materials. Although limited to its state, the Illinois law has been cited by many legal experts as a template for other federal and state laws.

Based on the Illinois law, employers who use AI during their hiring process should adopt the following best practices:

- Give notice to applicants of the use of AI-powered video-interview platforms;
- Explain what the AI is and how it works in ordinary language to applicants;
- Obtain consent of applicants to use and record their video interviews;
- Offer an alternative interview method for interviews; and
- Have a procedure in place for the destruction of recordings.

Drug and Alcohol Testing

Employers with drug and alcohol testing policies are highly regulated by the states where they operate. State requirements vary about required notice of testing, the nature and location of testing, and when testing may occur. All states protect employee privacy regarding who receives the test result and how those results are to be collected, stored, and destroyed. Employers who engage in drug and alcohol testing need to be informed about the legal consequences of enforcing their policies.

Employees frequently challenge drug and alcohol testing as a violation of their right to privacy. Employers generally win these lawsuits when:

- The employer complies with all state requirements for drug and alcohol testing;
- Conducts the test with the employee's consent;
- Conducts the test in a manner that was not offensive; and
- The test results do not reveal information unrelated to the purpose of the test.

Employers must be careful to limit disclosure of test results to only those with a need to know. Businesses may lawfully conduct a drug or alcohol test but still be liable for privacy violations based on how they handled the results.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) seeks to protect confidential health information and mandates standards for handling such information.

HIPAA has a Privacy Rule regulating the use and disclosure of individually identifiable health information. The Privacy Rule protects **Protected Health Information (PHI)**, which includes all information related to the past, present or future health status of an identified individual, of treatment received, or of payment for treatment. PHI also includes billing records, information about premium payments, and enrollment information. As a result, PHI includes medical information required by employers to carry out their obligations under the Americans with Disabilities Act, the Family Medical Leave Act, workers' compensation, drug testing, and employer-sponsored health care plans.

HIPAA also has a Security Rule to ensure the confidentiality, integrity and availability of electronic PHI. Under the Security Rule,

- **Confidentiality** means PHI is not made available or disclosed to unauthorized individuals or processes;
- **Integrity** means PHI is not altered or destroyed in an unauthorized manner; and
- **Availability** means PHI is accessible and usable upon demand by an authorized individual.

The Security Rule also requires businesses to protect electronic PHI against reasonably anticipated threats and reasonably anticipated violations of the Privacy Rule.

Figure 21.1 HIPAA Security Rule

C.I.A.



Technology Safeguard

- *Access Control*
- *Audit Control*
- *Integrity*
- *Person or Entity Authentication*

Physical Safeguard

- *Facility access controls*
- *Workstation use*
- *Workstation security*



Administrative Safeguard

- *Security management, security officer*
- *Workforce security, information, access management*
- *Training security incident*

Privacy Rule “Reasonable” Safeguard for all



HIPAA requires businesses to designate a single person who is ultimately responsible for the security of electronic PHI. This person is also responsible for ensuring the business engages in the mandatory security management process under HIPAA. This process starts with a risk analysis of the potential vulnerabilities in the business's system and management of PHI. The security management process is extensively regulated.

Importantly, HIPAA applies to “covered entities” rather than specific types of information. Personal fitness trackers such as Fitbit, gather what is essentially healthcare data of its consumers. However, Fitbit data can be sold as consumer information because Fitbit is not a covered entity under HIPAA with regard to its consumers. However, if Fitbit gathers PHI of its employees who request medical leaves of absence, then Fitbit is a covered entity as an employer.

Electronic Monitoring

Federal law and most state laws allow employers to monitor their employees' electronic communications occurring over the employer's hardware, software, and servers. If the employer provides the computer system, the employer has the right to monitor electronic communications on the system, even if those communications are not work related.

Employers may also monitor communications when employees consent to the monitoring. Therefore, many employers require employees to sign a waiver consenting to private communications sent via the employer's equipment to be monitored. This helps defend against invasion of privacy claims better than having a policy in the employee handbook alone.

Businesses may also monitor conversations with customers in the ordinary course of business as long as they give notice. As a result, many customer service lines use a recorded message that “this call may be monitored for training purposes” before customers are connected to a customer service agent.

The most important federal law regarding monitoring of electronic communications is the **Electronic Communications Privacy Act (ECPA)**, which was passed by Congress in 1986. ECPA has two parts. The first part is known as the Wiretap Act and the second as the Stored Communications Act. ECPA prohibits the acquisition of the the content of a wire, oral or electronic communication using an electronic, mechanical or other device. ECPA also prohibits the use or disclosure of an unlawfully intercepted communication.

ECPA exposes businesses to multiple levels of liability within a business. For example, personnel in the IT department may be liable for unlawfully intercepting an employee's email, and human resource personnel who use and disclose the email may be liable as well. Each unlawfully intercepted communication may give rise to liability. Therefore, a handful of communications may result in multiple individuals throughout a business repeatedly violating ECPA.

Workplace Recordings

Although recordings may be useful to capture the content of a conversation, recordings pose legal and business risks to employers. Both employers and employees may violate federal and state wiretapping laws by recording conversations without consent of the other parties. Even with consent, businesses that engage in recording employees and customers damage employee morale and risk losing customers.

Twelve states prohibit recording a conversation unless all parties consent. The majority of states allow customers and employees to hold a business liable for wiretapping violations under the respondeat superior doctrine. As a result, businesses may be liable for their employees' unlawful recordings if done in the course and scope of employment or done to help the business.

State and federal wiretapping laws carry both civil and criminal penalties. Many state laws provide for treble damages or a statutory damage amount. Federal wiretapping laws impose fines up to one hundred dollars per day or ten thousand dollars, whichever is greater.

Another potential problem for businesses is putting confidential business information at risk. For example, employees may capture trade secrets, proprietary information, or business strategies that the business wants to protect. Recorded information can be compromised or shared against the business's interests.

Social Media

An employer's right to monitor electronic communications generally does not include social media. As a result, employers are not entitled to monitor social media accounts through coercion or deceit. For example, an employer cannot require employees to provide passwords to their social media accounts. Employers also cannot log onto the social media accounts of others (including employees) and pose as them to see private accounts.

However, if social media accounts are public, then employers are entitled to review them to the same extent as other members of the public.

Videotaping and Surveillance Cameras

ECPA only protects electronic communications. As a result, ECPA does not apply to video or camera surveillance without an audio component. To avoid violating ECPA, businesses should ensure their security and surveillance cameras do not capture human voices.

Security cameras cannot be used in areas in which employees and customers have a reasonable expectation of privacy. For example, retailers cannot use cameras in changing rooms, restrooms, and locker rooms. Businesses need to place cameras so that private activity cannot, and is not, monitored and recorded.

Businesses engaged in surveillance must use the most limited means available to conduct the surveillance. Companies should have a legitimate business reason to use security cameras, and they need to ensure the surveillance is targeted and limited in duration and scope.

Retailers who use cameras to prevent theft at entryways and cash registers should place cameras in positions that are open and obvious to act as notice to customers. Signs giving express notice are also a best practice to avoid legal liability.

Biometrics and Wearable Technology

Biometrics is the automated identification of people using their physical characteristics. While many metrics can be used, fingerprints and facial recognition are the most common. It is helpful to think of biometrics as measurements of some aspect of a person.

There is a growing trend among businesses to move from traditional time clocks to biometric time clocks that scan fingerprints, retinas, or irises to verify an employee's identity and clock the employee in and out of work. Biometric time clocks prevent time clock fraud, increase timekeeping efficiency, and increase accuracy of wages.

The type of biometric technology used impacts the privacy rights involved. Technology storing biometric data directly impacts privacy rights more than technology creating a "template" through an algorithm to create a representation of a fingerprint. Whether the technology captures and uses existing personal information or creates a replica has legal consequences.

There have been a series of class action lawsuits against employers that have not notified employees when their biometric identifiers and data were being shared with third party timekeeping vendors. Consent is only a defense for employers if they give notice and obtain consent for all uses of the information.

Another technology trend is the use of wearable technology. **Wearable technology** is a category of electronic devices that can be worn as accessories, embedded in clothing, implanted in the user's body, or even tattooed on skin. The devices are intended to be hands-free, are powered by microprocessors and connect with the Internet. Wearable technology includes smartwatches, fitness trackers, and medical devices. It is helpful to think of wearable technology as something that an employee has.

Wearable technology is often used to track employee locations and grant access to areas. Concerned about private companies coercing employees to be microchipped, states are passing laws prohibiting employers to require, coerce, or compel an individual to receive a microchip implant or use wearable technology as a condition of employment.

11.3: Workplace Privacy is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.

- **21.3: Workplace Privacy** by [Melissa Randall and Community College of Denver Students](#) is licensed [CC BY 4.0](#). Original source: <https://introductiontobusinesslaw.pressbooks.com>.