Privacy in the Employment Relationship

by Thomas H. Wilson, Vinson & Elkins LLP and Corey Devine with Practical Law Labor & Employment

Maintained • USA (National/Federal)

This Practice Note provides an overview of privacy issues in employment, which may arise in various contexts, such as background checks, drug testing, email and other electronic surveillance and tracking by GPS. Invasion of privacy claims are highly fact-intensive and largely dependent on state law. This Note contains information that is general and not jurisdiction-specific.

Contents

Overview of Privacy Laws

Background Checks
- Background Checks Conducted Internally by the Employer
- Background Checks Conducted Externally by a Third Party

Employment Testing of Applicants or Employees
- Drug Testing
- Polygraph Tests
- HIV or AIDS Tests
- Medical and Physical Examinations
- Other Types of Testing

Employee Personnel Records
- Employee Medical Records
- Sensitive Personally Identifiable Information

Employee Electronic Communications
- Monitoring of Emails and Internet Usage
- Requiring Disclosure of Electronic Account Access Information
- Monitoring of Telephone Calls

Video Surveillance of Employee Behavior on the Job

Searching Employee Surroundings on the Job
- No Expectation of Privacy in Common Areas
- Employer Limits

Employees' Lawful, Off-Duty Activities

Tracking Employee Movements by GPS
Privacy Concerns
Consent and Notice
Other Considerations

Monitoring and Employee Rights Under the National Labor Relations Act

Information about Employees Relevant to Health and Safety

This Note provides a general overview of the key legal principles involved in employee privacy in the private employment context. It summarizes the patchwork of state and federal case law and statutes that regulate privacy in the workplace.

Specifically, this Note describes:

- Background check protocols, including appropriate use and legal requirements.
- Employment testing, including **tests** for drugs, alcohol, truthfulness and health conditions.
- Employee personnel records, including general rules of maintenance and access.
- Employee knowledge of and access to confidential business information, including steps to safeguard company information.
- Online and email activity by employees, including information on tracking, monitoring, notice, balancing of interests and legal risks.
- Searching employee workplace surroundings, including the limits of employer rights and best practices.
- Surveillance of employees at the workplace, including costs, benefits and legal limits.
- Off-duty employee activity, including a general discussion of state requirements.
- Tracking employee movement through technology, including commonly asked questions about the practice.
- Communication by employees about unionization, including law and best practices.
- Health and safety information about employees, including employee rights and risks to others in the workforce.

Overview of Privacy Laws

There is no federal legislation defining an employee's right to privacy in the private sector workplace. The US Constitution's Fourth Amendment prohibition against "unreasonable searches or seizures" applies to public employers and governmental action (See *O'Connor v. Ortega*, 480 U.S. 709 (1987)).

An employee's right to privacy in the private employment context is largely based on state law, which differs from state to state, and may arise under any of the following:

- The state's constitution.
- State statutes.
- The common law.

Privacy rights are implicated in numerous ways in the workplace, from conducting background checks to monitoring employees' emails. In analyzing whether an employee's right to privacy has been violated, courts generally consider whether:

- The employee had a reasonable expectation of privacy.
- The employer's actions intruded on an employee's reasonable expectation of privacy, and if so, to what extent.
- The employer had a legitimate business reason for its actions.

Courts balance these factors, weighing an employee's right to privacy in a particular context against an employer's business need for its actions. Critical to the analysis is whether the employer provided advance notice to employees about its practices and whether the employer's actions were overly invasive.

Background Checks

Employers may conduct background checks on employees before extending an employment offer, during the course of employment or both. Background checks are generally used to:

- Verify information provided on an employment application.
- Ensure that an applicant or employee has not been involved in criminal conduct, such as a crime involving:
  - immorality (also known as moral turpitude);
  - violence; or
  - financial misconduct.
- Investigate suspected criminal conduct, such as when an employer believes that a current employee has been charged with a criminal offense that impacts his ability to do his job.

An employer should obtain an applicant's or employee's consent before conducting a background check, as consent is an affirmative defense to an invasion of privacy tort claim. Different requirements apply, however, depending on whether the background check is conducted internally by the employer or externally by a third party.

Background Checks Conducted Internally by the Employer

If an employer intends to conduct the background check internally (that is, gather information themselves from publicly accessible records and information), some states only require that the applicant or employee sign a basic form indicating that he consents to the background check. In other states, such as California, employers that conduct background checks internally must comply with state law requiring certain disclosure, use and consent requirements (see State Q&A, Background Check Laws: California). For information about other states' laws, see Background Check Laws: State Q&A Tool.

Background Checks Conducted Externally by a Third Party

If an employer engages a third-party service to conduct the background check, in most cases it must ensure that it complies with the **Fair Credit Reporting Act** (FCRA), in addition to any analogous state laws.

The FCRA is a federal law that regulates the collection, dissemination and use of consumer information, including information such as credit ratings and criminal history (see 15 U.S.C. § 1681). The FCRA only regulates the use of information obtained from a consumer reporting agency. A consumer reporting agency is an entity that collects and disseminates information about consumers to be used for credit evaluation and certain other purposes, including employment-related purposes.

Entities that use information obtained from consumer reporting agencies for employment purposes, including background checks, must comply with the FCRA by:

- Obtaining the consumer's consent to conduct the background check using a consent form containing specific information required by the FCRA.
- Notifying the consumer when an adverse action is taken on the basis of a report obtained from a consumer reporting agency.
- Identifying the consumer reporting agency that provided the credit report so that the consumer may contest the accuracy and completeness of the report.

For more information on employee background checks and requirements of the FCRA, see Practice Note, Background Checks and References. For state-specific information on background checks, see Background Check Laws: State Q&A Tool.

Employment Testing of Applicants or Employees

Drug Testing

In addition to background checks, many employers, especially those in safety-sensitive industries, require employees to submit to drug and alcohol testing either before being hired, during employment or both.

Common reasons for drug testing include:

- Encouraging productivity in the workplace.
- Ensuring that employees can safely perform job duties.
- Investigating workplace accidents and incidents.

Pre-Employment Testing

Pre-employment drug testing is the most common. These programs require all job applicants to submit to and pass a drug screen as part of a conditional job offer.

The Americans with Disabilities Act of 1990 (ADA) and certain states allow employers to **test** employees for unlawful drugs before employment begins. However, because alcohol testing is considered a medical examination under the ADA, an employer cannot request a job applicant to undergo alcohol testing before a conditional job offer is made. Alcohol testing must be job-related and consistent with business necessity. Therefore, employers should take precautions when administering pre-offer drug **tests** to ensure that testing is narrowly-tailored and compliant with the ADA (see, for example, *EEOC v. Grane Healthcare Co. & Ebensburg Care Ctr., LLC, d/b/a Cambria Care Ctr.*, 2 F.Supp.3d 667 (W.D. Pa. 2014)). For other requirements, see Employee Drug and Alcohol Testing under the Americans with Disabilities Act Checklist: Pre-Employment Testing and Drug Testing Laws: State Q&A Tool: Question 2. As with most types of employment-related **tests**, an employer should both:

- Obtain an applicant's written consent to a pre-employment drug or alcohol **test**
- Advise the applicant, in writing, that passing the **test** is required to receive an offer of employment.

For more information, see Standard Document, Drug Testing in the Workplace Policy.

Drug Testing of Existing Employees

Drug and alcohol testing programs of existing employees may include:

- Testing on a periodic or randomized basis.
- Reasonable suspicion testing.
- Post-incident testing.
- Testing that is legally required in certain industries, such as Department of Transportation testing required in the trucking industry.

Prior to implementing any employee drug and alcohol testing program, an employer should develop and distribute to all affected employees a detailed drug and alcohol testing policy and procedure. The written materials should clearly explain the circumstances that trigger testing and the consequences of failing to submit to a **test** or failing a **test**. Employees and supervisors should receive formal training on the policy and its enforcement.

As with pre-employment testing, an employer should obtain written consent before requiring any employee to submit to a drug or alcohol **test**. See Standard Document, Drug Testing in the Workplace Consent Form. An employer with a unionized workforce should not implement a drug and alcohol testing program before bargaining, as these programs are generally considered mandatory subjects of bargaining (see Subjects of Collective Bargaining Chart).

Drug and alcohol testing programs are generally regulated by state law. Many states have statutes covering testing programs. Some states have voluntary statutes that apply only to those employers that wish to qualify for certain benefits, such as workers' compensation premium discounts. Additionally, a handful of cities, such as San Francisco, California, and Boulder, Colorado, have enacted city ordinances regulating drug and alcohol testing programs. In states (and cities) without testing statutes, drug and alcohol testing is usually regulated by case law.

Drug and alcohol testing laws typically address three main issues related to testing programs:

- Who may be tested and under what circumstances (in other words, pre-employment, random or for-cause testing).
- How testing is to be conducted.
- The technical testing standards that must be observed by the testing entity.

Most employers, even those that are large and sophisticated, opt to outsource drug and alcohol testing to a third-party service provider familiar with, and able to abide by, applicable technical testing requirements. Outsourcing also insulates an employer from some of the potential liability associated with a testing program, such as invasion of privacy claims. In some states, employers are required to use a state-licensed laboratory when drug testing its employees.

The following examples of key aspects of various state drug and alcohol laws demonstrate how these laws differ from state to state:

- In Connecticut, an employer must notify applicants if it requires pre-employment testing. Random testing may not be imposed on employees unless they work in safety-sensitive positions or if it is authorized under federal law. Post-incident testing is permitted only if there is a reasonable basis to suspect drug use. (Conn. Gen. Stat. §§ 31-51t to 31-51x).
- Nebraska has enacted a statute requiring, among other things, employers to comply with an employee's request for a blood **test** to confirm a positive breath **test** result (Neb. Rev. Stat. § 48-1903 (2)(b)).
- Rhode Island prohibits employers from terminating an employee after a first positive **test** result and instead requires that the employer refer the employee to substance abuse counseling or treatment (R.I. Gen. Laws § 28-6.5-1(a)(3)).

For information on drug testing in other states, see Drug Testing Laws: State Q&A Tool.

The Occupational Safety and Health Administration (OSHA) amended its recordkeeping standards in 2016 to include anti-retaliation provisions. The new anti-retaliation provisions do not expressly mention drug testing. However, the preamble to the final rule cites automatic post-injury drug testing as a form of adverse action that may discourage employees from reporting work-related injuries or illnesses, as drug testing is often perceived as invasion of privacy.

Therefore, OSHA takes the position that mandatory post-accident or injury testing may deter reporting unless:

- It is conducted only in situations where employee drug use is likely to have contributed to the injury or incident.
- The **test** used can accurately identify a present impairment, as opposed to drug use at some time in the recent past. This requirement has made many employer question whether post-accident or injury drug testing is ever permissible under OSHA's new anti-retaliation provisions. Although alcohol **tests** are capable of measuring an employee's present level of impairment, current drug testing protocols are not capable of doing so.

(See Improve Tracking of Workplace Injuries and Illnesses, 81 Fed. Reg. 29624-01, 29672-73 (May 12, 2016).) For more information about OSHA's anti-retaliation provisions, see Practice Note, Drug and Alcohol Use, Abuse, and Testing in the Workplace: Compliance with the OSH Act.

Although the ADA and similar state laws protect individuals who are in rehabilitation for drug and alcohol addiction, these laws do not protect use of illegal drugs in the workplace and, accordingly, do not regulate drug testing. For more information, see Employee Drug and Alcohol Testing Under the Americans with Disabilities Act Checklist.

In many states, drug and alcohol **test** results are considered confidential. For example, in Vermont, all information obtained regarding **test** results is considered strictly confidential and may be released only by voluntary written consent of the individual tested. The only exception is when release of the information is compelled by a court of competent jurisdiction in connection with an action under the drug-testing law. (Vt. Stat. Ann. tit. 21, § 516.)

Polygraph Tests

At one time, administering polygraph **tests** to employees was common practice for employers. But in 1988 Congress passed the Employee Polygraph Protection Act, which prohibits most private employers from using lie detector **tests** either for pre-employment screening or during the course of employment. (29 U.S.C. §§ 2001-2009 and 29 C.F.R. §§ 801.1-801.75).

HIV or AIDS Tests

The ability of employers to **test** the HIV or AIDS status of prospective or current employees is severely limited. The ADA prohibits HIV or AIDS testing to screen out job applicants. In addition to the ADA, most states have enacted laws addressing the use of HIV or AIDS testing. For example, in California, the use of HIV **tests** to determine suitability for employment is specifically prohibited (Cal. Health & Safety Code § 120980(f)). Employers who obtain an employee's medical information, including HIV or AIDS-related information, must keep the information confidential and prevent unlawful use and disclosure of the information (Cal. Civ. Code § 56.20 to 56.245).

In Texas, an employer may not require an employee to take a **test** for AIDS or HIV except "as a bona fide occupational qualification and there is not a less discriminatory means of satisfying the occupational qualification" (Tex. Health & Safety Code Ann. § 81.102(a)(5)(A)). The employer bears the burden of proving that the **test** is necessary (Tex. Health & Safety Code Ann. § 81.102(b)). An employer who obtains an HIV/AIDS **test** result regarding an employee must maintain such result in the strictest confidence (Tex. Health & Safety Code Ann. § 81.103). Under the statute, "**test** result" includes any statement that an identifiable person has or has not been tested for AIDS or HIV infection, including a statement that the person is positive, negative, at risk or has or does not have a specific level of antigen or antibody (Tex. Health & Safety Code Ann. § 81.101(5)). Disclosure, except under very limited statutory exceptions, can result in criminal penalty (Tex. Health & Safety Code Ann. § 81.103(j)).

Medical and Physical Examinations

Employers may not require a job applicant to submit to a medical or physical examination before making a conditional job offer.

Employers that obtain medical information about employees or prospective employees must comply with obligations to maintain the confidentiality of the information (see Medical Examination and Inquiries in Employment Checklist: Confidentiality). In addition to federal laws, state laws may also impose confidentiality obligations (see, for example, California's Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56-56.16).

Other Types of Testing

Employers may opt to utilize other types of **tests** in the employment context, such as psychological or **personality tests**. Employers must ensure these types of **tests** are not administered in a discriminatory manner and have a legitimate business reason. Results of these **tests** should also be maintained confidentially.

Employee Personnel Records

Federal law does not specifically regulate an employer's maintenance and handling of employee personnel records. Generally, employers should treat personnel files as confidential records belonging to the employer.

Personnel records should be maintained in a secure location, such as a locked file cabinet or password-protected electronic files. They should be made available only to individuals with a legitimate business need to access the files. This practice protects the confidential information contained in the files and limits the likelihood that inappropriate documents will be placed in the files.

Not all states have enacted laws specifically addressing employee personnel records. In some states, personnel records are generally considered to be the property of the employer and an employee has no legal right to access or review his personnel file. Other states, however, have enacted laws granting employees the right to access personnel records. These laws typically address:

- Who may access an employee's personnel records.
- When access must be granted.
- What information or records may be accessed.

The following are examples of laws that states have enacted to regulate access to personnel files:

- In Alaska, employees or former employees may inspect or make copies of their own personnel files. An employer is permitted to charge a reasonable fee for copying services. (Alaska Stat. § 23.10.430 (2009).)
- In California, every employee has the right to inspect personnel records relating to the employee's performance or any grievance. The employer must keep a copy of an employee's personnel records at the place where the employee reports to work. An employee must be granted access to his personnel files within a reasonable time after requesting to review the file. (Cal. Lab. Code § 1198.5.)
- In Delaware, an employer must permit an employee to inspect his personnel file at a reasonable time after receiving a request from the employee (Del. Code. Ann. tit. 19, §§ 730-735.)

- In Illinois, employees may request to view their personnel files, including reports used to determine qualifications for employment, promotion, transfer, additional compensation, discharge or disciplinary action. Employers can require that the request be in writing. (820 Ill. Comp. Stat. 40/2).

For more information, see Practice Note, Employee Access to Personnel Files State Laws: Overview.

Employee Medical Records

Although there is no overriding federal law governing personnel files, the ADA imposes strict rules for handling information obtained through post-offer medical examinations and inquiries, or through the **reasonable accommodation** process. Employers covered by the ADA must keep these types of medical records confidential and store them separate from other personnel records.

An employee's medical information may be revealed only to:

- Safety and first aid workers, if necessary to treat the employee or provide for evacuation procedures.
- The employee's supervisor, if the employee's disability requires restricted duties or a reasonable accommodation.
- Government officials as required by law.
- Insurance companies for the purpose of workers' compensation claims.

(42 U.S.C. § 12112(d)(3)(B), 42 U.S.C. § 12112 (4)(C), and 29 C.F.R. § 1630.14(b)(1).)

For more information, see Medical Examination and Inquiries in Employment Checklist: Confidentiality.

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA) and the **Genetic Information Nondiscrimination Act of 2008** (GINA) also impose on most employers the obligation to maintain employees' health-related information in a confidential manner. Accordingly, employers, even those that are not covered by the ADA, should treat all employee medical or health information as private and confidential. For more information about requirements under GINA, see Practice Note, Discrimination under GINA: Basics.

Certain states, such as California, require employers who receive medical information to maintain appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of the information (Cal. Civ. Code §§ 56.20-56.245).

Sensitive Personally Identifiable Information

With identity theft on the rise, many states have begun protecting individuals' social security numbers and other personally-identifiable information.

Laws Protecting Social Security Numbers

In addition, a number of states, including Alaska, California, Connecticut, Hawaii, Illinois, Kansas, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, New Mexico, New York, Oklahoma, Oregon, Pennsylvania, South Carolina, Texas, and Utah have enacted specific protections regarding the use and disclosure of employee Social Security numbers. See Alaska Stat. §§ 45.48.400 to 45.48.480, 45.48.500 to 45.48.590; Cal. Lab. Code § 226; Conn. Gen. Stat. §§ 42-470 & 42-471; Haw. Rev. Stat. §§ 487J-1 to 487J-3; 815 Ill. Comp. Stat. § 505/2RR; Kan. Stat. Ann. § 75-3520; Mass. 201 C.M.R. 17; Md. Code Ann., Lab. & Emp. § 3-502; Mich. Comp. Laws §§ 445.82 to445.86; Minn. Stat. § 325E.59; Mo. Rev. Stat. § 407.095; Neb. Rev. Stat. § 48-237; N.M. Stat. Ann. 57-12B-4; N.Y. Lab. Law § 203-d; Okla. Stat. tit. 40, § 173.1; Or. Rev. Stat. §§ 646A.620, 646A.622, & 646A.624; Pa. Stat. Ann. tit. 74, §§ 201& 204; S.C. Code Ann. §§ 37-20-110, 37-20-180 & 37-20-200; Utah Code Ann §§ 34-46-301 & 34-46-302.

For example, New York law restricts an employer's use and dissemination of social security numbers and other personally identifiable information. Specifically, employers may not, unless otherwise required by law:

- Publicly post or display an employee's social security number.
- Visibly print a social security number on any identification badge or card, including a time card.
- Place a social security number in a file, such as a personnel file, with unrestricted access.
- Communicate an employee's "personal identifying information" to the general public.

(N.Y.S. Lab. Law § 203-d; N.Y. Gen. Bus. Law § 399-ddd(4).)

"Personal identifying information" is defined broadly to include an employee's:

- Social Security number.
- Home address.
- Home phone number.
- Personal email address.
- Internet ID or password.
- Parent's surname prior to marriage.
- Driver's license number.

The New York statute also prohibits the use of social security numbers as identification numbers for the purposes of any occupational licensing.

Employers in states that have no laws regulating the use and dissemination of social security numbers and personally identifiable information should still consider adopting practices to safeguard this information to protect against invasion of privacy claims.

Laws Governing Security Breach Notification

Additionally, accidental disclosure of data containing personally identifiable information may trigger an employer's obligation to comply with notification requirements under security breach notification laws. These data security laws, enacted in most states within the past decade, are designed to respond to the dramatic rise in the number of breaches of consumer databases containing personally identifiable

information leading to identity theft. For more information, see Practice Note, Privacy and Data Security: Breach Notification. Employers that maintain personally identifiable information about their employees in computerized data are covered by most security breach notification laws.

California, one of the first states to enact a security breach notification law, requires any person or business in the state that owns or licenses computerized data that includes personal information to comply with certain disclosure and notice requirements if the unencrypted information is, or is reasonably believed to have been, acquired by an unauthorized person (Cal. Civ. Code § 1798.82). As of January 1, 2017, the law also cover's any person or California-based business that owns or licenses encrypted personal information when the encryption key or security credential used to unencrypt the date is also obtained by an unauthorized party (Ca. Civ. Code § 1798.82).

Under the California statute, personal information is defined as either of the following:

- An individual's first name or initial, plus the last name, in combination with one or more of the following items, when either the name or the following items are not encrypted or encrypted if the encryption has been breached:
  - social security number;
  - driver's license number or California Identification Card number;
  - account number, credit or debit card number, in combination with a security code or password that would enable access to an individual's financial account;
  - medical information; or
  - health insurance information.
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(Cal. Civ. Code § 1798.82.)

The breach notification laws enacted in many other states are modeled on California's law. For additional information on state-specific data breach law, see Practice Note, Privacy and Data Security: Breach Notification: Overview of State Data Breach Notification Laws and State Agency Notice Requirements for Data Breaches Chart.

Employee Electronic Communications

A growing number of employers track their employees' electronic communications, including phone calls, emails and internet usage while at work. Employers cite a number of reasons for these types of monitoring, including to:

- Maintain employee productivity and minimize personal use of the employer's telephone and computer systems.
- Ensure compliance with workplace policies and procedures, such as policies prohibiting sexual harassment.
- Monitor and prevent disclosures of confidential business information.
- Protect the employer's reputation.

The federal **Electronic Communications Privacy Act** (ECPA) protects the privacy of wire, oral and electronic communications including:

- Telephone.
- Email.
- Internet communications.

(18 U.S.C. §§ 2510-2522.)

Employers are subject to the requirements of the ECPA but generally may monitor employee telephone calls and computer usage under various exemptions.

Monitoring of Emails and Internet Usage

Federal law permits employers to monitor employees' internet or email usage as long as:

- The information is stored on employer-provided wire or electronic communications services.
- The review is authorized by the employer's own policies.

For more information, see Practice Note, Electronic Workplace Monitoring and Surveillance: Stored Communications Act.

For example, the Eleventh Circuit recently ruled that a manager had violated the Stored Communications Act when he accessed an employee's email without the permission of senior management and based "solely on suspicion of dishonesty concerning the content of communications between others, without any reason to suspect wrongful or illegal conduct prior to doing so." (*Brown Jordan International, Inc. v. Carmicle*, 846 F.3d 1167, 1177-78 (11th Cir. 2017).)

Only two states, Delaware and Connecticut, require employers to provide written notice to employees before electronically monitoring their activities (see Del. Code tit. 19 § 705 and Conn. Gen. Stat. Ann. § 31-48d). However, in Connecticut, an employer's failure to do so does not provide a private cause of action under the statute (*Gerardi v. City of Bridgeport*, 985 A.2d 328 (2010)). Colorado and Tennessee require only public entities to adopt written policies regarding electronic monitoring activities. (Colo. Rev. Stat. § 24-72-204.5; Tenn. Code §10-7-512.)

Challenges to this type of monitoring are often based on common law invasion of privacy claims alleging that the employer's monitoring has intruded upon the employees' seclusion. Generally, the employee must establish:

- The employer intentionally intruded on the employee's solitude, seclusion or private affairs.
- The intrusion would be highly offensive to a reasonable person.
- The employee suffered an injury as a result of the employer's intrusion.

(See *Valenzuela v. Aquino*, 853 S.W.2d 512 (Tex. 1993).)

Courts generally consider an employer's monitoring of an employee's computer activity to be an intentional intrusion. Workplace invasion of privacy claims typically hinge on whether the intrusion would be highly offensive to a reasonable person. To prevail on an intrusion upon seclusion claim, an

employee typically must show that he had a reasonable expectation of privacy regarding his emails and online usage while using the employer's computer systems in the workplace.

Notice and Expectation of Privacy

In these types of cases, courts typically determine the boundaries of an employee's reasonable expectation of privacy in his emails and online usage and balance those expectations against the employer's business interests in monitoring employee computer activity.

Different courts may consider and weigh various factors, including:

- The general nature of the work environment.
- The employer's stated justification for its monitoring.
- The employee's interest in protecting his activity or information.
- The means of monitoring utilized by the employer.
- The reasonableness of the employee's expectation of privacy in the context.
- Whether the employer:
  - gave notice to employees of its policy or practice of monitoring its electronic and computer systems and the extent of monitoring; or
  - allowed or disallowed employees to use its computer systems for personal use, or limited it to business use only.

Providing written notice to employees regarding the employer's monitoring of all its electronic and communications systems is the primary method of notifying employees that they should have limited or no expectation of privacy when using the employer's computer systems. Most employers include a policy in their employee handbook expressly advising all employees about the proper use of its communications systems (whether it's strictly limited to business use or can be used from time to time for personal usage), and that the employer may, and routinely does, monitor its electronic communications and computer systems. For a sample policy, see Standard Document, IT Resources and Communications Systems Policy.

Legal Risks

Maintaining and disseminating written notice of its electronic monitoring policy does not insulate an employer from legal risk. Courts examining the issue of an employee's expectation of privacy have reached differing results under similar circumstances. For example:

- The New Jersey Supreme Court ruled that an employee had a reasonable expectation of privacy in emails she sent to her attorney using a personal, password-protected web-based Yahoo email account, even though she used the employer's laptop to send and receive those messages and the employer had an electronics communication monitoring policy in place. The policy did not specify that employees' use of personal, web-based email accounts accessed through the employer's equipment could be viewed, or that the contents of those emails could be forensically retrieved and read by the employer. (*Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010).)

- A California appellate court ruled that an employee had no reasonable expectation of privacy in her personal emails and in fact had waived the attorney-client privilege when she used her employer-provided email account to email her attorney after she had been warned that the account was to be used for business only and that the employer would randomly monitor account activity. (*Holmes v. Petrovich Dev. Co.*, 191 Cal. App. 4th 1047 (2011).)
- Following the *Stengart* decision, a New Jersey appellate court ruled that, although the company lacked any email policy, the employee had waived the attorney-client privilege by failing to password-protect his emails and by sending them from the employer's email account (see *Fazio v. Temporary Excellence, Inc.*, 2012 WL 300634, (N.J. Super. Ct. App. Div. Feb. 2, 2012)).

A comprehensive electronic communications policy that makes clear that personal web-based email accounts may also be viewed by the employer if accessed from company property would arguably notify the employee that there should be no expectation of privacy in that context.

Aside from invasion of privacy claims, employers monitoring employee emails and Internet activity potentially face other claims, including:

- **Labor issues.** By monitoring online activity such as posts on social networking websites or employee email traffic, an employer may unwittingly learn about employee **concerted activity** that is protected by the **National Labor Relations Act** (NLRA) (29 U.S.C. § 157). Under the NLRA, an employee fired for posting comments on Facebook or other social media could file an **unfair labor practice** charge and may be entitled to reinstatement with back pay if he proves that the social media postings resulting in termination constituted protected concerted activity (see Standard Document, Social Media Policy: Drafting Note: Compliance with the NLRA). For more information, see Monitoring and Employee Rights Under the National Labor Relations Act.
- **Discrimination claims.** If an employer's monitoring activities at work reveal employees' protected characteristics, employees may claim protection under anti-discrimination statutes, including:
  - **Title VII of the Civil Rights Act of 1964** (Title VII).
  - The **Age Discrimination in Employment Act of 1967** (ADEA).
  - The ADA.

However, unless a protected characteristic is hidden or unknown to an employer (as in the case of some disabilities), it may be difficult for an employee to prevail on such a claim. Employers should not apply their monitoring policies in a discriminatory way, for example, by disciplining female employees more severely than male employees for engaging in similar conduct, such as posting on a personal blog mildly provocative photos while wearing work uniforms as it could lead to claims of sex discrimination (see, for example, *Simonetti v. Delta Airlines, Inc.*, 2005 WL 2407621 (N.D. Ga. Sept. 7, 2005)).

For more information, see Practice Note, Electronic Workplace Monitoring and Surveillance: Employment Discrimination Laws.

Requiring Disclosure of Electronic Account Access Information

The following states now bar employers from seeking login information from employees or applicants for personal electronic accounts, including social media accounts:

- Arkansas.
- California.
- Colorado.
- Connecticut.
- Delaware.
- Illinois.
- Louisiana.
- Maine.
- Maryland.
- Michigan.
- Montana.
- Nevada.
- New Hampshire.
- New Jersey.
- New Mexico.
- Oklahoma.
- Oregon.
- Rhode Island.
- Tennessee.
- Utah.
- Virginia.
- Washington.
- Wisconsin.

For example, in Maryland, employers cannot:

- Request or require that an employee or applicant disclose user names, passwords or other means for accessing personal accounts or services through an electronic communications device.
- Discharge, discipline or otherwise penalize an employee, or threaten to do so, for the employee's refusal to disclose protected login information.
- Fail or refuse to hire an applicant as a result of the applicant's refusal to disclose protected login information.

(Md. Code Ann., Labor and Empl. § 3-712.)

For more information, see Practice Note, Employer Access to Social Media Accounts State Laws: Overview. Congress and additional states, including Massachusetts, Georgia and New York, are considering similar measures.

Monitoring of Telephone Calls

Some employers may wish to monitor employees' telephone calls. For example, employers may want to record calls to ensure:

- The quality of customer service calls.
- That personal calls are not being excessively made.

Employers who wish to monitor employee telephone conversations should include in their workplace monitoring policy details about the telephone monitoring program. All employees must be notified that telephone conversations may be monitored, and the employer should obtain written consent to monitoring.

The federal Wiretap Act, as amended by the ECPA, prohibits the interception of communication using electronic, mechanical or other means. Monitoring employee telephone calls can constitute an unlawful interception under the Wiretap Act, but employers are often exempted from the requirements by one or more statutory exceptions (see Practice Note, Electronic Workplace Monitoring and Surveillance: Exceptions to the Federal Wiretap Act).

Employers must also comply with state law, however, and should confirm that telephone monitoring is legal in their jurisdiction. In at least twelve states, the consent of all parties to a telephone conversation is required before the conversation may be recorded. These states are:

- California.
- Connecticut.
- Delaware.
- Florida.
- Illinois.
- Maryland.
- Massachusetts.
- Michigan (Michigan appellate courts have interpreted the all-party consent rule as applying only to conversations the recorder is not involved in. See *Sullivan v. Gray*, 342 N.W.2d 58, 60-61 (Mich. Ct. App. 1982)).
- Montana.
- New Hampshire.
- Nevada (two-party consent is required for telephone or wire communications; only one-party consent is required to record in-person conversations).
- Pennsylvania.
- Washington.

For more information, see Practice Note, Electronic Workplace Monitoring and Surveillance.

Video Surveillance of Employee Behavior on the Job

With some exceptions, employers are generally permitted to monitor employee activity in the workplace through video surveillance. The benefits of video surveillance are that it can:

- Increase employee productivity.
- Improve workplace security.
- Decrease theft and other inappropriate behavior in the workplace.

Employers that implement video surveillance programs must be careful to avoid inadvertently invading employees' privacy rights. Employers should advise employees that video surveillance equipment is in use in the workplace and that workplace activities may be monitored and recorded. Prior to engaging in video surveillance of its employees, employers should:

- Implement a video surveillance policy that includes:
  - a statement that the employees consent to video surveillance in the workplace by accepting and continuing employment with the employer;
  - the appropriate uses of the video surveillance;
  - the employees who have access to surveillance footage; and
  - disciplinary consequences of improper use of video surveillance.
- Obtain employees' written consent to video monitoring in the workplace.

Video surveillance equipment should be installed only in those areas in which employees have no expectation of privacy, such as:

- Lobbies.
- Hallways.
- Workrooms.

Employers should not monitor private spaces such as:

- Restrooms.
- Changing areas.

Some states have enacted laws restricting the areas that can be monitored. For example:

- In California, it is illegal to monitor a wash room, shower or locker room (Cal. Lab. Code § 435(a)).
- In Connecticut, it is illegal to monitor spaces meant for employee rest and comfort, such as employee break rooms (Conn. Gen. Stat. Ann. § 31-48b)).

Video cameras generally should be visible so that employees can determine which areas of the workplace are subject to monitoring. An employer also should consider posting notice in all rooms or areas in which video surveillance equipment is in use. As a general rule, video surveillance equipment should capture only video, and not audio. An employer who uses surveillance equipment to capture audio may violate federal wiretapping laws (see 18 U.S.C. § 2512).

Searching Employee Surroundings on the Job

Employers have the right to search an employee's workspace, including their desk and office in most circumstances. The workspace is furnished by, and belongs to, the employer, and courts have generally found that employees do not have an expectation of privacy in these areas.

Whether an employee has an expectation of privacy in specific areas in the workplace is a case-by-case inquiry based on a number of factors, such as:

- The characteristics of the location claimed by the employee to be private. For example, whether it is:
  - a shared hallway;
  - a locked office;
  - an employee parking garage; or
  - other space.

- The employer's stated practice with respect to workplace searches.
- The employer's actual practice with respect to workplace searches.
- The employer's stated reason for the workplace search.

No Expectation of Privacy in Common Areas

Most courts have found that an employee has no expectation of privacy in common workplace areas such as lobbies, hallways, and workrooms.

Courts have also found that employees have no expectation of privacy in their locked office when the employee is aware that the employer maintains a key to the office or otherwise has the ability to access the office. This is true even if the office contains goods of a private or personal nature. For example, in *Peitsmeyer v. Jackson Township Bd. of Trs.*, the Ohio Court of Appeals affirmed summary judgment in favor of the employer where the alleged invasion of privacy consisted of the employer entering the employee's locked office, unlocking desk drawers, and searching a storage locker and discarding the employee's personal belongings, including personal and sensitive items related to the employee's son's legal troubles (2003 WL 21940713 (Ohio Ct. App. Aug. 14, 2003)). A similar result can be expected when an employee claims an expectation of privacy in an employer-provided desk or closet.

Employer Limits

An employer's right to search an employee's workspace is not without bounds. For example, at least one court has held that an employee may have an expectation of privacy in his briefcase even though he abandoned it in his former employer's office (see *Branan v. Mac Tools*, 2004 WL 2361568, *11-12 (Ohio Ct. App. Oct. 21, 2004)). The court reasoned that the briefcase was the employee's personal property and that the employee had no reason to expect that the employer would access it.

Similarly, a Texas state court held that an employee may have an expectation in an employer-provided locker where the employee supplied her own lock and had no reason to believe that the employer had any means of accessing the locker once it was locked (see *K-Mart Corp. v. Trotti*, 677 S.W.2d 632, 637-38 (Tex. Ct. App. 1984)).

If an employer plans to conduct searches of an employee's workspace, it should advise the employee in writing at the time of hiring that the employee should have no expectation of privacy in the workplace. A policy should, as specifically as possible, outline all areas controlled by the employer that are subject to search. An employer also should obtain written consent to workplace searches from each employee.

Even if an employer has obtained consent to a search, however, it should be cautious when searching or monitoring areas in which an employee may claim to have a reasonable expectation of privacy. Such areas include:

- Employee lockers or places where personnel effects are stored (particularly when such spaces are locked with an employee-furnished lock).
- Employee vehicles (though there may be a justification if it is on employer property).
- Employee handbags, briefcases or other personal effects.

When possible, the employer should obtain employee consent to the specific search to be conducted. For example, if an employer expects that an employee has illegal drugs in her purse, it should ask for authorization to search the purse. If the employee withholds consent, in most states, the employer is free to terminate the employee and there is no risk of an invasion of privacy claim.

Employees' Lawful, Off-Duty Activities

An employee's right to engage in certain lawful, off-duty activities is protected by a wide variety of state laws. At least twenty-nine states and the District of Colombia have enacted statutes protecting employees from discrimination or retaliation based on their participation in recreational or leisure-time activities during their personal time. For example, some of these state laws protect employees from discrimination or retaliation for:

- **Tobacco use.** Statutes in the District of Columbia and the following states specifically protect the use of tobacco:
  - Connecticut;
  - Indiana;
  - Kentucky;
  - Louisiana;
  - Maine;
  - Mississippi;
  - New Hampshire;
  - New Jersey;
  - New Mexico;
  - Oklahoma;
  - Oregon;
  - Rhode Island;
  - South Carolina;
  - South Dakota;
  - Virginia;
  - West Virginia; and
  - Wyoming.
- **Using consumable goods.** Statutes that protect lawful use of consumable products, including tobacco as well as other consumable products, generally have been enacted in states such as:
  - Illinois;
  - Minnesota;
  - Missouri;
  - Montana;
  - Nevada;
  - North Carolina;
  - Tennessee; and
  - Wisconsin.
- **A broader range of lawful off-duty conduct.** States with statutes that protect broader types of lawful activities that employees engage in while off-duty (which may include protection for tobacco use or use of other consumable goods and expressive, online activities such as blogging or participating in discussions on internet message boards) include:

- California;
- Colorado;
- New York; and
- North Dakota.

These statutes protecting lawful off-duty conduct vary in the extent of their provisions.

For example, North Dakota's statute broadly prohibits employers from discriminating against employees for "participation in lawful activity off the employer's premises during nonworking hours" (N.D. Cent. Code § 14-02.4-01). The provision contains two important exceptions. Employees are not protected when participation in the activity is either:

- Contrary to a bona fide occupational qualification that reasonably relates to the employment duties of a particular employee or group of employees, rather than to all employees of that employer.
- In direct conflict with the essential business-related interests of the employer.

Subject to certain exceptions, New York prohibits discriminating against any individual for engaging in certain activities during non-working hours, off-premises and while not using the employer's equipment or property, including:

- political activities;
- legal use of consumable products;
- legal recreational activities; and
- union membership.

(N.Y. Lab. Law § 201-d; see State Q&A, Anti-Discrimination Laws: New York)

Connecticut's statute differs from those of other similar states' laws in that it prohibits disciplining or discharging an employee who exercises the right to free speech, as long as the activity does not "substantially or materially interfere" with either:

- The employee's job performance.
- The employer and employee's working relationship.

(Conn. Gen. Stat. Ann. § 31-51q.)

Employers that take adverse employment action against an employee for lawful off-duty conduct may face liability, even in states that have not enacted a statute specifically protecting this conduct. Several states, such as California, New Mexico, and Virginia recognize the tort of wrongful termination in violation of public policy. An employee may argue that his discharge for engaging in lawful activity violates state public policy.

Many states have also legalized the use and possession of marijuana for medicinal purposes. Two states, Colorado and Washington, have legalized the drug for recreational use. However, marijuana remains an illegal drug under federal law, which has led to confusion in these states regarding an employer's right to discipline an employee who **tests** positive for marijuana during a workplace drug **test**. Most recently in Coats v. Dish Network, LLC, 350 P.3d 849 (Co. 2015), the Colorado Supreme Court held that although an employee's medical marijuana use outside the workplace was licensed under Colorado state law, it was unlawful under the federal law. As a result, the employee's termination for violation

of the employer's drug policy was not protected under Colorado's "lawful activities" statute (Colo. Rev. Stat. Ann. § 24-34-402.5).

For more information on state laws on marijuana use, see Practice Note, State Medical and Recreational Marijuana Laws: Overview.

Tracking Employee Movements by GPS

Advanced technology now enables employers to monitor their employees' movements and locations in various ways. For example, Global Positioning System (GPS) devices use satellite technology allowing employers to track the movements and locations of employees in real time almost anywhere. Employers are able to do so through GPS devices that are typically located in employer-issued property, such as:

- Smartphones or mobile phones.
- Navigation systems in company cars.
- GPS devices that may be placed in company cars.

Not all employers monitor their employees using GPS technology available to them. Employers who do might monitor employees to:

- Ensure employee safety and security.
- Track the use of employer resources.
- Increase employee productivity.

Privacy Concerns

The use of GPS technology to track employees' locations and movements raises significant privacy concerns. Unlike traditional forms of surveillance, GPS can be particularly invasive because of the amount of detail and data that are tracked and the possibility of intruding into an employee's private life. For example, an employer that uses GPS to monitor an employee's use of a company-issued car may track the employee's movements during both personal and business time.

Employers that have attempted to implement GPS monitoring programs often experience significant pushback from employees. In the case of unionized employers, the use of GPS monitoring may be challenged as an unfair labor practice and an invasion of privacy (see, for example, *Haggins v. Verizon New England, Inc.*, 736 F. Supp. 2d 326 (D. Mass. 2010)).

Even nonunionized employers may be subject to claims that monitoring with GPS infringes on employee rights to engage in protected concerted activity under the NLRA (see Monitoring and Employee Rights Under the National Labor Relations Act).

Consent and Notice

There is limited case law directly addressing a private employer's right to use GPS monitoring in the workplace. At least one court has found that the placement of a GPS device in a vehicle provided by an employer is not an unreasonable intrusion of employee privacy (see *Elgin v. St. Louis Coca-Cola Bottling Co.*, 2005 WL 3050633 (E.D. Mo. Nov. 14, 2005)). Coca-Cola installed GPS devices in its employees' vehicles, without notifying its employees, to investigate a theft. Since the employees were also allowed to use those vehicles while off duty, one of the drivers who had been cleared of suspicion sued the employer for violating his right to privacy. The court ruled that since the company owned the vehicles and the GPS tracking did not reveal anything other than what was already public, such as the location of the vehicle, the GPS tracking did not constitute any significant invasion of the employee's privacy.

A recent US Supreme Court case also addressing GPS tracking, although in the criminal context, held that the police's actions in secretly placing a GPS device on a car registered to the wife of a suspect was a warrantless search in violation of the suspect's Fourth Amendment rights (see *United States v. Jones*, 132 S. Ct. 945 (2012)).

Though the Fourth Amendment does not apply to private employers, the case suggests that employers who wish to monitor their employees with GPS undertake certain precautions, such as:

- Notifying employees that they are subject to monitoring if they use company-issued property installed with GPS.
- Informing employees that they should have no expectation of privacy as to their location and whereabouts when using company property installed with GPS.
- Obtaining the written consent of employees to be monitored by GPS on company-issued devices. In most jurisdictions, consent is an affirmative defense to tort claims and can eliminate or reduce the risks associated with a GPS monitoring program. Some states, such as California, have laws that restrict the manner in which employers can monitor employees without consent.
- Verifying that their GPS surveillance programs comply with local legal requirements.
- Limiting their monitoring of employees to work time to avoid intruding on employees' personal lives outside of working hours.

Other Considerations

Before implementing a GPS monitoring program, an employer should also consider the following:

- **Is GPS surveillance truly necessary?** Employers are often quick to embrace technology that increases productivity, but they should consider the risks associated with a GPS surveillance program. Improperly used, GPS technology can expose an employer to a variety of legal claims, including tort claims for invasion of privacy that carry punitive damages. Because of these risks, employers should consider whether GPS surveillance is truly necessary, such as to:
  - maintain a mobile workforce that must be closely monitored; or
  - minimize or eliminate safety risks to which the the employer's workforce is routinely exposed.

- **What effect, if any, might GPS surveillance have on employee morale?** A drawback to GPS technology is that employees subject to monitoring may feel that their employers do not trust them. Others may become defensive and work less effectively when they know the employer may be watching their every move. Employers should not discount the potential psychological effects of GPS monitoring on employee morale.

- **How will the implementation of the GPS surveillance program be communicated to employees?** From an employee-relations standpoint, the biggest pitfall is a failure to properly communicate with employees about implementation of the program. Employers that implement monitoring programs should consider communicating directly with employees before surveillance begins about:
  - the purposes of monitoring;
  - how monitoring will be conducted;
  - who will be privy to historical monitoring data; and
  - the possible uses of such data.

- **How will expectations regarding the proper uses of GPS surveillance be communicated to management?** One of the most significant legal risks associated with GPS surveillance is its misuse. Employers should establish policies defining the limits of its surveillance program, the proper uses of surveillance data and the individuals who will have access to the data. Supervisors should be trained on the employer's surveillance policy and be required to advise senior management of any suspected misuse of surveillance information.
- **What details regarding a surveillance program should be provided to employees in a GPS monitoring policy?** A GPS surveillance program is only effective if it functions as intended, allowing an employer to monitor and locate employees as necessary for business purposes. Most GPS-capable devices such as mobile phones, however, have limitations. A phone's GPS functionality may be disabled or an employee may turn her phone off completely except for limited times such as when making calls or checking voice-mail. Accordingly, a GPS monitoring policy should explain to employees the logistics of the monitoring program, including the times during which employees are expected to carry GPS-enabled tracking devices and the times during which employees may (or must) deactivate such devices. The policy should also clearly explain the disciplinary consequences of disabling a GPS device during working time without a business justification.

Monitoring and Employee Rights Under the National Labor Relations Act

Monitoring employees in the workplace raises specific concerns under the NLRA. The NLRA prohibits employers from taking certain actions against employees who engage in concerted activities for the purpose of either:

- Collective bargaining.
- Other mutual aid or protection.

(29 U.S.C. § 157.)

These protections apply to non-supervisory employees in both unionized and nonunionized workplaces (see *NLRB v. Phoenix Mut. Life Ins. Co.*, 167 F.2d 983, 988 (7th Cir. 1948)). For more information, see Practice Note, Employee Rights and Unfair Labor Practices Under the National Labor Relations Act.

For an employee's conduct to be "concerted," he must act with, or as authorized by, other employees. The definition of concerted activity includes situations where an individual employee seeks or attempts to initiate, induce or prepare for group action (see *Meyers Indus., Inc.*, 281 N.L.R.B. 882, 887 (1986)). Further, concerted activity is found when an employee's action is a "logical outgrowth" of previous group activity (see *Every Woman's Place, Inc.*, 282 N.L.R.B. 413, 413 (1986)).

Concerted activities are only protected when undertaken for "mutual aid or protection" (29 U.S.C. § 157). The NLRB has historically interpreted this to mean that employees must undertake concerted activity for a "self-interested economic objective," such as improved pay, hours, safety or workload.

The NLRB has consistently held that surveillance of employees engaged in concerted activity is an unfair labor practice (see *Consol. Edison Co. v. NLRB*, 305 U.S. 197 (1938) and *Cook Family Foods*, 311 N.L.R.B. 1299 (1993)). This is the case even if employees are not aware that they are under surveillance (see *NLRB v. J.P. Stevens & Co.*, 563 F.2d 8 (2d Cir. 1977), cert. denied, 434 U.S. 1064 (1978)).

Employers must be sensitive to employees' rights to engage in protected concerted activities and must not implement monitoring programs that infringe on those rights. For example:

- An employee may file an unfair labor practice charge and be entitled to reinstatement with back pay if he can prove that an employer's GPS monitoring resulted in his termination in violation of his right to engage in concerted activity. Employees can also file a charge against an employer to stop surveillance of concerted activity. GPS surveillance could easily be used to monitor, even unwittingly, an employee's visits to the local union hall.
- Video surveillance of employee break areas may capture employees engaged in protected concerted activity such as discussing wages, hours of work or other terms and conditions of employment.
- An employee's complaints about working conditions that are posted on Facebook can be protected concerted activity, though the analysis is fact-intensive and there is developing case law on this topic. For more information, see Practice Note, Disciplining Employees for Social Media Posts in View of the NLRA .

In drafting and implementing surveillance programs, employers should take care not to violate the NLRA (see Standard Document, Social Media Policy (US)). Overly broad surveillance likely infringes on employee opportunities to engage in concerted activities and are therefore unfair labor practices under Section 8(a)(1) of the NLRA.

Information about Employees Relevant to Health and Safety

Occasionally, an employer's interest in promoting a safe working environment may conflict with an employee's personal privacy interests. This is particularly true in situations involving outbreaks or epidemics of highly infectious diseases such as the swine flu (H1N1 virus). Employers must carefully balance employee privacy rights with company health concerns in these situations.

Before taking any action to address an employee health issue, an employer must consider the confidentiality obligations imposed by the ADA and HIPAA, as well as analogous state and federal laws. Generally, an employer must maintain the confidentiality of employees' health information and restrict disclosure to those employees who have an absolute need to know the information. For more information, see Practice Note, Pandemic Flu Preparation and Response: Medical Privacy Issues and Confidentiality Obligations.

If an employer becomes aware that an employee may be infected with a disease that poses a threat to the health and safety of other employees, it should:

- Approach the potentially infected employee and address the situation directly. The employer should not rely on rumors regarding the employee's situation.
- If an employee confirms exposure to a highly infectious disease that poses a threat to other employees, request written consent to disclose the information to co-workers. In many jurisdictions, consent is a defense to an invasion of privacy claim.
- If disclosure of an employee's health issue is necessary, avoid using information identifying the employee. A generalized notice that an employee may have been exposed to an infectious disease is adequate in almost all cases.
- Train all employees, especially supervisors, on confidentiality obligations with respect to employee medical issues. Employers should also adopt a policy prohibiting discrimination or retaliation against an employee infected with a disease.

For more information, see Medical Examination and Inquiries in Employment Checklist: Confidentiality.

