11 Common Workplace Privacy Issues (and 4 Common-Law Claims)

Only a *Reasonable* Expectation

It is important to remember that employees have only a *reasonable* expectation of privacy. Employers can lower the threshold of what is considered reasonable by developing a clear policy addressing workplace privacy issues and communicating the policy to their employees.

Private Employees Enjoy Relatively Little Freedom

Several states have enacted statutory or constitutional provisions guaranteeing their citizens the right to privacy from certain intrusions. In the absence of a state constitutional provision or existing law, however, private employees enjoy relatively little freedom from workplace intrusion. Therefore, private employees must look to common, or judge-made, law to find privacy protections.

Four Common-Law Privacy Claims

There are essentially four common-law privacy claims that are available to private employees. These are:

1. **Intrusion into an individual's private solitude or seclusion.** An employee may allege this form of privacy invasion when an employer unreasonably searches (e.g., a locker or desk drawer) or conducts surveillance in areas in which an employee has a legitimate expectation of privacy (e.g., dressing rooms). An employer's improper questioning of an employee (e.g., sexual habits or orientation) may also give rise to this type of claim.

2. **Public disclosure of private facts.** An employee may claim this form of privacy invasion when an employer publicly discloses private and, arguably, embarrassing facts about an employee to a wide audience without his or her permission.

3. **Portraying an individual in a false light.** Under this theory, if an employer attributes a false or offensive conduct or characteristic to an employee that is not true (e.g., criminal activity), the employee may claim invasion of privacy.

4. **Use of an individual's name or likeness.** When an employer uses an employee's photograph or likeness, or attributes specific statements to an employee without his or her permission, an individual may have a valid misappropriation claim (e.g., the employer publishes an employee's photograph or likeness on company brochures without first obtaining the employee's consent).

Constitutional Guarantees

Public employees. Public employees are also protected by the U.S. Constitution. The U.S. Supreme Court has held that there is a federal constitutional right to personal privacy. Thus,

public employers must be very careful to avoid practices that infringe upon their employees' reasonable expectations of privacy as guaranteed by the Constitution.

11 Common Workplace Privacy Issues

In the employment setting, there are unfortunately a number of areas in which an employer's practices might ultimately violate an employee's privacy rights. Although the following summary outlines the more important existing federal regulations and general rules that may restrict and affect employer activities, remember to check state laws and constitutions.

1. Physical Searches

An employer's search of an employee's person or private belongings is perhaps the most intrusive form of employer inquiry. However, a physical search may be warranted and lawful under certain circumstances. For example, if a jewelry store videotape shows that an employee is stuffing jewelry in his or her pockets without paying for it, the employer may be justified in conducting a limited physical search of the employee. (But remember that a public employer's right to conduct searches is limited by the Fourth Amendment's prohibition on unreasonable search and seizure.)

2. Video Surveillance

An employer may have a legitimate business interest in videotaping its employees; however, to avoid running afoul of an employee's privacy rights, employers should *only* videotape in open or public areas in which there is a diminished or no expectation of privacy (e.g., shop floor), and the employer should give its employees notice that they are being videotaped.

3. Background and Credit Checks

The federal Fair Credit Reporting Act (FCRA) requires employers to obtain applicants' consent when a third party conducts a background investigation. Some states also have their own background check laws.

4. Internet and E-Mail

The Electronic Communications Privacy Act of 1986 (ECPA) prohibits the unlawful and intentional interception of any wire, oral, or electronic communication (*18 USC 2510 et seq.,18 USC 2701 et seq.*). Title II of ECPA, the Stored Communications Act (SCA), also prohibits access to such information while in electronic storage.

There are three broad statutory exceptions that might prove useful to employers. The provider exception, the business-use exception, and the prior-consent exception.

5. Social Networking Sites

Employees have increasingly been utilizing social networking sites for a variety of uses, both personal and professional. Although these sites can be beneficial, their use can also have risks, such as the following:

- **Discrimination.** By viewing candidate profiles, employers may learn more information (e.g., race, disability, age, religion, family/marital status, sexual orientation) than the employer could legally ask about directly.
- **Background check laws.** It is unclear whether federal FCRA and some state laws would require consent from an applicant before an employer or third party conducted an Internet search as part of a background check. However, even if not legally required to do so, employers should consider getting consent so that applicants are on notice that the information they post on social networking sites may be reviewed by the employer.
- **Monitoring employee use of social networking sites.** There is little case law addressing employers monitoring employees' social networking posts. However, the few cases in this area suggest that courts will be reluctant to uphold an invasion of privacy claim—whether based on the U.S. Constitution or state common law—when an employee voluntarily posts information on a public site.
- **Right to organize.** Another possible concern for employers that monitor employee use of social networking sites is the National Labor Relations Act (NLRA), which protects employees' right to engage in a concerted activity regarding terms and conditions of employment.

6. Social Media/Personal Internet Account Privacy

After news media reports that some employers were requiring job applicants and existing employees to provide access to their social media accounts, many state and federal lawmakers have proposed (and several states have passed) legislation to ban this practice.

7. Genetic Information

The Genetic Information Nondiscrimination Act (GINA) prohibits employers from discriminating against employees or applicants on the basis of genetic information. The law applies to all public employers, private employers with 15 or more employees, employment agencies, and labor organizations.

8. Medical Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created national standards to protect individuals' medical records and other personal health information and to give patients more control over their health information.

9. Alcohol and Drug Testing

Many employers maintain drug- and alcohol-free workplaces. Note that state and federal law may limit or regulate the employer's ability to do drug testing and, if tests are permitted, to maintain the privacy of results in a specified manner.

10. Legal and Recreational Activities Outside the Workplace

As noted earlier, many states have enacted laws protecting employees from adverse employment action based on their lawful conduct outside the workplace.

11. Social Security Numbers (SSNs)

In an effort to thwart the growing tide of identity and credit theft cases, a number of states have passed legislation governing the manner in which employers and other individuals handle SSNs.