



Privacy

©2009 eNotes.com, Inc. or its Licensors. Please see [copyright information](#) at the end of this document.

- [Background](#)
- [Federal Law Governing Workplace Privacy](#)
- [State Law Governing Workplace Privacy](#)
- [Conclusion](#)
- [Additional Resources](#)
- [Organizations](#)

Background

Employers have a legitimate and important interest in maintaining an efficient and productive workforce and a safe workplace. Most employers establish rules governing workplace conduct to ensure that employees stay on task and earn their wages. Yet, these rules are often broken, and that in turn increases the need for employers to monitor their employees. Prior to the present era of technology and computers, employer supervision typically took the form of hands-on monitoring, a supervisor patrolling the workplace to make sure that employees were doing their jobs. In some employment settings hands-on supervision remains common place. For example, many manufacturers still employ supervisors to monitor assembly-line workers as they toil each day. In a host of other employment settings, human supervision has been replaced at least in part by technological supervision.

Technological innovations, particularly computers, have drastically altered the nature of the employer-employee relationship. Where once a human supervisor could only monitor employee activity in one place at one time, networked computers now allow employers to monitor nearly everything, nearly all the time, and without employees knowing whether they are being watched. Internet usage can be monitored by employers seeking to compile data about the websites being visited by their employees. Files stored on employees' hard drives can be scanned for format and content. Surveillance cameras can monitor workers' activity throughout the workplace. Telephone lines can be monitored and telephone conversations recorded.

There are two kinds of workplace electronic surveillance, quantitative and qualitative. One type involves monitoring records and analyzes quantitative information, such as the number of keystrokes per hour and the number of minutes spent on the telephone each day. The other type of monitoring analyzes the quality of performance in whatever qualitative terms an employer defines. For example, many employers monitor the content of incoming and outgoing email to make sure the messages exchanged are work-related.

Balanced against employers' interests in maintaining an efficient, productive, and safe workplace are employees' interest in privacy. Workers have a legitimate and important interest in being able to perform their jobs without fear of embarrassment or stigma that might result from an employer's unreasonable intrusion into their workspace. It is also reasonable for employees to expect that their employers will not disclose personal information they obtain via pre-employment applications, honesty tests, [POLYGRAPH](#) examinations, criminal background checks, urine or blood analyses, and the like.

The interests of employers and employees are not always at odds. The quality of the work environment is a concern to both groups. Employees do not generally appreciate having to worry about constant electronic

surveillance. Respect for employee privacy is one factor people consider when deciding whether to apply for a job, take a job, or keep a job, and employers generally take heed of this reality. Consistent with employers' goal of maintaining a productive workforce is their goal of attracting good employees and keeping them happy. Accordingly, most employers understand that they must offer a professional work environment in which employees can exercise a certain amount of liberty free from the watchful eye of a supervisor. However, the line separating a reasonable intrusion on employee privacy from one that is unreasonable is often neither clear nor bright, and courts are routinely asked to draw the line for labor and management as a whole.

In the United States the right to privacy traces its origins to the nineteenth century. In 1890 Samuel D. Warren and Louis D. Brandeis published "The Right to Privacy" (4 Harv. L. Rev. 193), an influential article that postulated a general [COMMON LAW](#) right of privacy. Before publication of this article, no U. S. court had ever expressly recognized a right to privacy. Since the publication of the article, courts have recognized a general right to privacy that Americans enjoy to varying degrees in different contexts.

Today privacy in the labor context is regulated at both the state and federal levels by a combination of constitutional provisions, federal statutes, and common law. Depending on the [JURISDICTION](#), the laws can regulate both private employees and public employees (i.e., employees working for a governmental entity). Companies doing business in multiple states must stay familiar with the privacy laws in each state.

Federal Law Governing Workplace Privacy

Federal law governing workplace privacy generally falls into two categories, constitutional law or [STATUTORY](#) law. There is no federal common law governing workplace privacy, other than the [CASE LAW](#) interpreting the U. S. Constitution and federal statutes.

Federal Constitutional Law

The Fourth Amendment to the U. S. Constitution prohibits the federal government from conducting unreasonable searches and seizures, and searches or seizures conducted without a [WARRANT](#) are presumptively invalid. The U. S. Supreme has repeatedly held that public employees are protected by the strictures of the Fourth Amendment precisely because they are employed by the government. *O'Connor v. Ortega*, 480 U. S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987). Workers employed by private companies enjoy no such constitutional protection.

The Supreme Court and lower courts have also consistently ruled that the Fourth Amendment right protecting public employees from unreasonable searches and seizures conducted by their employers is more limited than the right protecting the rest of society from searches and seizures conducted by law enforcement officials investigating criminal activity. The Fourth Amendment only protects individuals who have a "reasonable expectation of privacy" in the place to be searched or the thing to be seized. However, in the public employment context courts have recognized that they must balance the alleged invasion of an employee's privacy against the employer's need for control of a smoothly running workplace.

One consequence of this balancing is that employers typically do not need a [SEARCH WARRANT](#) or [PROBABLE CAUSE](#) to search an employee's work space, so long as the search is for work-related reasons. Even when the search is for [EVIDENCE](#) relating to employee misconduct, the employer's intrusion need not be made pursuant to a search warrant or probable cause unless the alleged misconduct rises to the level of criminal activity, at which point the employee is entitled to full protection of the Fourth Amendment.

Thus, it is generally recognized that most work-related intrusions by an employer comply with the Fourth Amendment's reasonableness requirement. Courts have said that requiring a warrant for work-related searches would be disruptive and unduly burdensome. To ensure the proper, ongoing operation of governmental agencies, entities, and units, courts interpret the Fourth Amendment as giving public employers wide latitude to enter employee offices, search their desks, and open their drawers and file cabinets for work-related reasons.

Drug testing of government employees (or of private employees pursuant to government regulation) has been addressed by several courts. Upon weighing the competing public and private interests, most lower courts have concluded that such testing is constitutional at least in those instances where the employer possessed a reasonable suspicion that a particular employee was using drugs and that the drugs affected the employee's job performance. For example, employers can compel workers to undergo blood, breath, or urine tests to check for drug use following a serious workplace accident that injured or imperiled others, so long as the employer has reason to believe that the accident was caused in part by an employee's drug use. Courts allowing drug testing in these situations have emphasized that the reasonable suspicion test fairly accommodates employees' privacy interests without unduly compromising workplace safety or the safety of the public.

Federal Legislation

For certain employees, drug testing is not only constitutionally permissible, but statutorily mandated. Under the Federal Drug-Free Workplace Act of 1988, drug testing is required of both public and private employees who are engaged in work that creates high risks of danger to the health and safety of other workers or the health and safety of the public. 41 U.S.C.A. sections 701 et seq. Employees targeted for mandatory drug testing include those employed in the following industries: mass transit, motor carriers (taxi cabs and buses), aviation, railroads, maritime transportation, and natural gas and pipeline operations. In addition, the Americans with Disabilities Act (42 U.S.C.A. section 12210) and the Rehabilitation Act of 1973 (29 U.S.C.A. sections 701 et seq) allow employers to establish drug testing programs for former drug users who are currently enrolled in a drug rehabilitation program or have completed one in the past. Because courts have interpreted these laws as effectively placing former and present substance abusers on notice, employees subject to their provisions typically understand the very limited privacy rights they enjoy when it comes to employer-mandated drug tests.

Less clear cut is the application of the National Labor Relations Act (NLRA) to privacy issues in the employment setting. The NLRA guarantees employees the right to "self-organize, to form, join, or assist labor organizations, to bargain collectively . . . and to engage in other concerted activities for . . . mutual aid or protection." 29 U.S.C.A. sections 101 et seq. The act also prohibits employers from committing "unfair labor practices" that would violate these rights. An [UNFAIR LABOR PRACTICE](#) is any action or statement by an employer that interferes with, restrains, or coerces employees in the exercise of their rights to self-organize.

Employer surveillance of employee activities may constitute an unfair labor practice if the surveillance interferes with, restrains, coerces, or intimidates employees who are exercising one of their rights protected by the NLRA. At the same time, the NLRA permits employers to enforce company rules aimed at guaranteeing employee productivity and safety, and federal courts have acknowledged that workplace surveillance is sometimes necessary to achieve these objectives. However, employee surveillance will not normally withstand scrutiny under the NLRA unless a rule is actually in place before the surveillance begins.

Once a rule is in place, the lawfulness of a particular surveillance method will be evaluated on a case-by-case basis. Where union or non-union employees conduct their activities openly on or near company property, employers may lawfully observe their activities without running afoul of the NLRA, even if there is no pre-existing rule in place authorizing such observation. *N.L.R.B. v. C. Mahon Co.*, 269 F.2d 44 (6th Cir. 1959). However, an illegal intent may be inferred from an employer's surveillance of open activities if the

surveillance is combined with other forms of employer harassment, interference, or intimidation, and the employee under surveillance is subsequently discharged. A history of anti-union animus will also weigh against an employer who is engaged in what would otherwise be deemed lawful surveillance. Conversely, what otherwise might be deemed an unfair labor practice can be made lawful if the surveillance is isolated, not accompanied by a threat, and the employer gives assurances that the employee's job is safe.

Before conducting surveillance of its employees, employers also need to familiarize themselves with the Omnibus Crime Control and Safe Streets Act of 1968. Pub.L. No. 90-351, 82 Stat. 197, June 19, 1968; 18 U.S.C.A. sections 2510-2520. Title III of the act prohibits any person from intentionally using or disclosing information that has been knowingly intercepted by electronic surveillance without consent of the persons under surveillance. As originally conceived, the act applied only to the "aural" acquisition of information by recording, bugging, [WIRETAPPING](#), or other devices designed to intercept and transmit sound.

Congress updated the act by passing the Electronic Communications Privacy Act of 1986 (ECPA). Pub.L. 99-508, Title I, Oct. 21, 1986, 100 Stat. 1848. ECPA governs the interception of data transmissions, which comprise the bulk of modern electronic communications. ECPA prohibits anyone from intercepting, accessing, or disclosing electronic communications without first getting authorization from the parties to the communication. However, ECPA does permit employers to monitor employees' electronic communications if the monitoring is done in the regular course of business, regardless of whether the communication involves a data or sound transmission, so long as the employer is the provider of the communication system being monitored. Thus, an employee's use of intra-company email is generally fair game for employers' to monitor. However, employees who transmit messages from work via a third-party email provider, such as Yahoo!, may create a reasonable expectation of privacy that insulates their communications from employer monitoring.

State Law Governing Workplace Privacy

State law governing workplace privacy generally falls into one of three categories, constitutional law, statutory law, or common law. Like their federal counterparts, state courts are cognizant of every employer's need to maintain an efficient, productive, and safe workplace. Nonetheless, state law often affords more protection for the privacy interests of both public and private employees,

State Constitutional Law

Many state constitutions guarantee a right to privacy independent of the right to privacy found in the federal constitution. Those states include Alaska, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, Texas, and Washington. Some of these state constitutional provisions apply only to public sector employees, while others have been interpreted to apply generally to all state residents. Although it is difficult to make meaningful generalizations about each of these state constitutional provisions, employees' privacy interests are frequently afforded greater protection under state constitutional law than they are under the federal constitution.

For example, the Texas Supreme Court invalidated a state agency's mandatory polygraph testing policy on the grounds that it violated the employee's privacy rights protected by the Texas constitution. *Texas State Employees Union v. Texas Department of Mental Health & Mental Retardation*, 746 S.W.2d 203 (1987). The court found that the test was "highly offensive" to the average employee because of the extremely personal nature of the questions asked. The court also concluded that the test was not accurate enough to provide a reliable way of identifying misbehaving, inefficient, or unproductive employees.

A California court reinstated a railroad employee who was fired for refusing to take a random drug test. The

court noted that an employee's right to privacy in refusing a drug test is not absolute under the state constitution but must be weighed against the employer's competing interests. *Luck v. Southern Pac. Transp. Co.*, 218 Cal. App. 3d 1, 267 Cal. Rptr. 618 (1990), rehearing denied 489 U.S. 939, 112 L. Ed. 2d 309, 111 S. Ct. 344 (1990). Conceding that the employer had a compelling interest in maintaining a safe workplace, the court noted that the discharged employee was simply a clerk who had no direct involvement with the railway operations. As a result, the court determined that the employee's privacy interests were more substantial than the employer's countervailing interests.

At the same time, state courts are pragmatic. They are normally disinclined to interpret a general right to privacy as a guarantee of specific individual freedoms that might be exercised to disrupt the workplace or interfere with an employer's legitimate interest in gathering relevant information about employees and job applicants. Thus, the Florida Supreme Court rejected a prospective employee's claim that she was not required to disclose whether she was a smoker on a pre-employment application. *City of North Miami v. Kurtz*, 653 So.2d 1025 (1995). The court found that the applicant did not enjoy a reasonable expectation of privacy regarding her use of tobacco.

State Legislation

Several states and U. S. territories have enacted statutory provisions that prohibit employers from spying on employees who are exercising certain protected rights. They include Connecticut, Hawaii, Kansas, Minnesota, New York, Rhode Island, the Virgin Islands, and Wisconsin. Most of the prohibitions contained in these statutes closely mirror or expand upon the prohibitions contained in the NLRA. Specifically, the statutes regulate employer surveillance of workers who are engaging in union-related activities, and each [STATUTE](#) permits employer surveillance that is done pursuant to clearly defined rules and in furtherance of legitimate business objectives.

A number of states have also enacted statutes that prohibit employers from disclosing certain personal information about employees gathered during the employment relationship. Minnesota, for example, forbids public employers from disclosing information contained in an employee's personnel file. M.S.A. sections 13.01-13.99. Georgia makes it unlawful for employers to obtain certain criminal history information about an employee or prospective employee without that person's consent. OCGA section 35-3-34(A). Alaska makes it unlawful for employers to require employees or job applicants take a polygraph [EXAMINATION](#). Alaska Stat. Section 23.10.037. However, no state prohibits an employer from requiring an employee or job applicant to undergo a psychological evaluation for the purpose of assessing the test-taker's propensity for truthfulness or deceit.

Several states limit the right of healthcare providers to release medical information to a patient's employer. For example, a Maryland statute generally requires the patient's consent before healthcare providers can disclose medical information to employers. Md Health General Code Ann., section 4-305. Similar statutory restrictions in Maryland prohibit insurance carriers from disclosing medical information to an insured's employer without the insured's consent. Md. Ins. Code Ann., section 4-403.

State Common Law

The state common law of torts generally recognizes three discrete rights of privacy that are regularly asserted during employment [LITIGATION](#). First, the common law affords individuals the right to sue when their seclusion or solitude has been intruded upon in an unreasonable and highly offensive manner. Second, individuals have a common law right to sue when information concerning their private life is disclosed to the public in an extremely objectionable fashion. Third, tort liability may be imposed on individuals or entities who publicize information that places someone in a false light.

A valid cause of action for invasion of privacy will not arise for any of these common law torts unless the employer's intrusion is so outrageous or pervasive as to offend the sensibilities of the average, reasonable person. Merely calling an employee at home, for example, will not give rise to a claim for invasion of privacy, unless the employer making the calls is doing so in a persistent and extremely offensive manner. *Johns v. Ridley*, 245 Ga.App. 710, 537 S.E.2d 746 (Ga.App. 2000). However, a claim for invasion of privacy may be supported by the allegations of female employees who claim that their supervisor has poked holes in the ceiling to watch them disrobe in the women's restroom. *Benitez v. KFC Nat. Management Co.*, 305 Ill.App.3d 1027, 714 N.E.2d 1002, 239 Ill.Dec. 705 (Ill.App. 2 Dist. 1999).

At the same time, an employer who merely reveals an employee's credit problems to co-workers may not be held liable for invasion of privacy. *Dietz v. Finlay Fine Jewelry Corp.*, 754 N.E.2d 958 (Ind.App. 2001). Nor may an employer be held liable for common law invasion of privacy by circulating a sexually suggestive photograph of a male employee, if the photograph accurately depicts the employee in a place open to the public. *Branham v. Celadon Trucking Services, Inc.*, 744 N.E.2d 514 (Ind.App. 2001). Similarly, an employer does not invade an employee's privacy during an office meeting by suggesting that the employee stole from the employer, if the employer's suggestion is made during an investigation of office thefts and the employee's possible role in them. *Zielinski v. Clorox Co.*, 215 Ga.App. 97, 450 S.E.2d 222. (Ga.App. 1994)

Conclusion

It is telling that much of the law governing privacy in the workplace actually protects employers from liability for invasion of privacy claims brought by employees. In this way the law reflects a general understanding among the American public that the workplace is essentially a place for commerce, productivity, and human interaction, but normally not a place for privacy or seclusion.

For the most part, employees themselves realize that the employer owns the company and expends the resources to make it profitable. Employees generally want to be efficient and productive so they can receive better reviews and better raises. Consequently, the law gives employers wide latitude and ample discretion in dictating how their businesses will be run. On the other hand, an individual does not abandon his or her privacy rights at the employer's front door. Instead, the law puts in place certain checks to prevent employers from overstepping **BOUNDARIES**, abusing their positions of power and authority, and running their businesses in a manner deemed highly offensive or objectionable to the average person.

Additional Resources

American Jurisprudence. West Group, 1998.

West's Encyclopedia of American Law. St. Paul: West Group, 1998.

Organizations

American Bar Association

740 15th Street, NW, Floor 8
Washington, DC 20005-1019 USA
Phone: (202) 662-1000
Fax: (816) 471-2995
URL: <http://www.abanet.org>

Encyclopedia of Everyday Law: Privacy

Primary Contact: Robert J. Saltzman, President

Electronic Privacy Information Center

1718 Connecticut Avenue, NW, Suite 200

Washington, DC 20009 USA

Phone: (202) 483-1140

Fax: (202) 483-1248

URL: <http://www.epic.org>

Primary Contact: Marc Rotenberg, Executive Director

National Lawyers Association

P.O. Box 26005 City Center Square

Kansas City, MO 64196 USA

Phone: (800) 471-2994

Fax: (202) 662-1777

URL: <http://www.nla.org>

Primary Contact: Mario Mandina, Chief Executive Officer

National Organization of Bar Counsel

515 Fifth Street, N.W.

Washington, DC 2001-2797 USA

Phone: (202) 638-1501

Fax: (202) 638-0862

URL: <http://www.nobc.org>

Primary Contact: Barbara L. Margolis, President-Elect

Copyright Notice

©2009 eNotes.com, Inc.

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution or information storage retrieval systems without the written permission of the publisher.

For complete copyright information, please see the online version of this work:

<http://www.enotes.com/everyday-law-encyclopedia>