J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 9(1) 3-12, 2000-2001

PRIVACY RIGHTS IN THE WORKPLACE: CONSTITUTIONAL AND STATUTORY CONSIDERATIONS

PAUL KOVATCH
Widener University School of Law at Harrisburg, Pennsylvania

ABSTRACT

The growth of surveillance in the workplace has increased at an alarming rate during the last decade. Various electronic and other surveillance techniques—including the use of video cameras, e-mail monitoring, telephone recordings, and searches of employee computers and cubicles—allow employers a seemingly unlimited ability to "keep tabs" on their employees. Such technological advances significantly affect the privacy rights of employees. This article examines how privacy rights at the workplace are treated constitutionally and statutorily. The author argues that employers' growing abuse of this ability to monitor employees and violate their right to privacy requires an examination of current protections for employees and, possibly, new solutions.

Technological advancements have played a major role in the workplace by greatly enhancing the employers' ability to monitor virtually every aspect of a worker's activities. The American Management Association reports that nearly two-thirds of its members conduct some form of electronic monitoring or surveillance of their employees [1, p. 825]. Employees and job applicants are increasingly subject to monitoring, including office and cubicle searches, video surveillance, electronic mail monitoring, and health and psychological screening [1, p. 826; 2, pp. 989, 1017]. Because this technology allows surreptitious surveillance, the employee's right to privacy may be almost entirely eliminated [1, p. 827; 3, pp. 1898, 1903]. The growing threat such surveillance poses to commonly accepted notions of privacy requires us to take a closer look at workplace privacy protections for private sector employees [1, p. 827; 4, pp. 102-104]. This article briefly traces the history of an employee's right to privacy, examines some of the current privacy laws, and explores some new privacy proposals and solutions to this growing issue of workplace monitoring.

A distinction must be made between public and private employment. Because constitutional rights usually protect citizens from the government, employees can claim a constitutionally protected right only if a state action occurs. Therefore, constitutionally protected rights can usually be secured only when the government is the employer. Because of this dichotomy, public sector employees enjoy greater privacy rights than do private sector employees. Private sector employer action rarely constitutes state action, so the typical private sector employee can find legal protection from intrusive employer surveillance only through claims brought under various state statutes or the common law tort of invasion of privacy. These remedies vary widely from jurisdiction to jurisdiction, and in some cases have not protected employees against even the most outrageous forms of employer intrusion [1, p. 829; 5, at *7].

HISTORY OF THE RIGHT TO PRIVACY

It is very difficult to define the term privacy [1, p. 832; 6, pp. 10-12]. No single definition or theory can capture all the nuances of the concept. Privacy in this article means: freedom from unwarranted and unreasonable intrusions into activities that society recognizes as belonging to the realm of individual autonomy [1, p. 833; 7, p. 7].

While there is no "right to privacy" found in any specific guarantee of the Constitution, the U.S. Supreme Court has recognized that "zones of privacy" may be created by more specific constitutional guarantees [8]. For example, in *Roe v. Wade,* the Court pointed out that the guarantee of personal privacy must be limited to rights that are "fundamental" or "implied in the concept of ordered liberty," such as matters relating to marriage, procreation, contraception, family relationships, child rearing, and education [8, 9]. As a result of *Roe* and many other cases, privacy has come to be regarded as a fundamental right. This country's historic respect for privacy has helped creativity and individuality flourish [1, p. 834; 10, pp. 1434-1438; 11]. American culture has been built on its "rugged individualism," diversity, and the willingness to accept challenges that test American creativity [12]. However, these traits may be sacrificed if privacy is not protected.

While individuals have a fundamental interest in privacy, they also have an obvious need to obtain and maintain employment [1, p. 834; 13]. Increasingly, however, a growing number of employers are resorting to intrusive monitoring techniques. These techniques force employees to sacrifice their privacy expectations because of their need to work. A very large number of cases have arisen from employer monitoring. Some of the alleged violations include videotaping changing rooms, timing bathroom breaks, random monitoring of phone conversations, or intercepting electronic mail [1, p. 826; citing 2, pp. 989, 1017]. Employers typically try to justify employee monitoring by citing increased worker productivity, better evaluation of work performance, deterrence of dishonesty, and limiting liability. But regardless of whether these interests are valid or are

done in good faith, employee monitoring creates increased stress, and often make employees feel demeaned.

A two-year study by the University of Wisconsin found that workplace monitoring causes physical and emotional health problems in employees [14, pp. 1256, 1262]. The study found a higher incidence of headaches and other physical ailments, such as backaches and wrist pain, among monitored workers [14, p. 1263]. Moreover, monitored workers also suffer greater fatigue. Psychological problems included a 12 percent increase in depression and a 15 percent increase in extreme anxiety [14, p. 1263].

CURRENT PRIVACY LAWS

What can employees do when they believe their privacy rights have been violated? In practical terms, the employee has little choice but to grin and bear it, or "simply" change jobs [15, p. 441]. However, people have certain expectations of privacy in their persons and effects. These expectations are protected to some degree by various legal provisions, including the U.S. Constitution, state constitutions or statutes where applicable, and common law [15, p. 728]. The extent of legal protection for a person's privacy is governed, in large part, by what the law considers to be "reasonable."

Privacy Under the U.S. Constitution

The Fourth Amendment to the U.S. Constitution protects privacy, in part, by prohibiting those acting under government authority from conducting unreasonable search and seizures. An unreasonable search is one in which an individual's reasonable expectation of privacy in what is being searched outweighs the government's need to conduct the search and obtain information. Typically, however, only public sector employees can invoke the Fourth Amendment protection against unreasonable searches and seizures to challenge employer searches of employees and property.

Private sector employees who wish to contest employer invasions of privacy must rely on a patchwork of federal and state statutes, common-law tort theories, and the public policy exception to the employment-at-will doctrine [15, p. 839]. Under these laws, the protection granted private sector employees is far less than the protection available to government employees. The courts have, however, applied a Fourth Amendment analysis to both public and private sector employees to determine whether the employee has a privacy right.

In 1987, the U.S. Supreme Court considered what constituted a reasonable search by a public employer under the Fourth Amendment [16]. In *O'Connor v. Ortega,* the Court analyzed whether the employer's search of a publicly employed psychiatrist's office and files was unreasonable [16]. The Court laid out an analytical framework to guide the lower courts when deciding whether a public

employer's justification for carrying out a search outweighs an employee's privacy interest in his/her offices and files [16].

The Court found that both public and private employees have a reasonable expectation of privacy [16, at 716]. However, one's expectation of privacy may be reduced by "actual office practices and procedures, or by legitimate regulation" [16, at 717]. In *O'Connor,* the target of the search was Ortega's office. The Court concluded that Ortega had an expectation of privacy because he did not share the office or files, he had occupied the office for seventeen years, and the employer did not discourage keeping personal items in the office [16, at 718-719].

The next element of the Court's analysis involved balancing "the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace" [16, at 719-720]. The Court initially noted that requiring employers to obtain a search warrant before conducting a search would be unworkable [16, at 720-722]. The Court stated that, because work-related searches promote efficiency, employers should have greater latitude to conduct such searches [16, at 723].

When balancing an employers' interest in efficiency and regulating employee conduct against an employee's expectation of privacy, the Court identified two issues that should be addressed [17, pp. 695, 730]. First, a court must consider whether the search was initially justified by reasonable suspicion that the search would turn up evidence of what the searchers were seeking [17, p. 730]. Second, the scope of the search must not go beyond that justified by the initial reason for searching [17, p. 730].

Thus, under *O'Connor,* three primary considerations exist in determining whether a search of a public employee's workplace is permissible under the Fourth Amendment [17, p. 730]. First, does the employee have a reasonable expectation of privacy in the thing to be searched [17, p. 730]? Second, does the employer have a reasonable, work-related need or suspicion to search [17, p. 730]? Finally, the scope of the search must not exceed what is necessary to investigate the employer's need or suspicion [17, p. 730].

However, because Ortega was employed at a state hospital and was considered a state employee, he was permitted to bring a Constitutional claim. As mentioned above, this right is rarely extended to private sector employees. Only the California courts have clearly held that the state constitutional right to privacy applies with respect to both public and private employers [14, pp. 1256, 1265]. In other states, employees have successfully invoked the state constitutional right to private only after establishing that the government was the employer [14, pp. 1256, 1265].

Pennsylvania provides an example of the path more frequently taken by the states. Article I, section 8, of the Pennsylvania Constitution contains language almost identical to that of the Fourth Amendment. Similar to that amendment, Article I, section 8, extends to searches conducted by public officials or those acting on their behalf. However, the search-and-seizure clause of the Pennsylvania

Constitution may be more comprehensive than the Fourth Amendment. The courts have noted that the protection of individual privacy against reasonable governmental search and seizures under the Pennsylvania Constitution are more expansive than those afforded under the U.S. Constitution [18]. However, the courts have not afforded private sector employees any constitutional protection.

STATUTORY PROTECTIONS

Federal

The federal legislation most relevant to employee privacy is Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act (ECPA) of 1986 [1, pp. 825, 839; 19]. The ECPA, with certain exceptions, prohibits any interception or disclosure of oral, wire, and electronic communications, or any entry into an electronic system to alter or obtain stored communications [1, p. 840]. However, because of the following exceptions, the ECPA provides very limited protection of employee privacy. The ECPA does not require prior notice to employees of monitoring. Consent to monitoring need not be expressly given, and it can be inferred from an employee's awareness of the monitoring [1, p. 840]. Among the factors relevant to establish awareness are whether the employee was generally informed that calls will be monitored and the manner in which the monitoring will take place. In addition, the business-extension exclusion of the ECPA exempts interceptions made by equipment "furnished to the subscriber or user by a communications carrier in the ordinary course of business and being used by the subscriber or user in the ordinary course of business" [1, p. 840]. The only limitation the law imposes on monitoring employee communication is that the surveillance be "within the ordinary course of business" [1, p. 841, citing 20]. It is difficult to imagine how any monitoring scheme that enhances productivity or efficiency would not be construed as "within the ordinary course of business" [1, p. 841; 21]. Finally, what limited protection the ECPA might afford employees has been greatly weakened because the statute quickly became outdated [1, p. 841; 22, pp. 345-347]. The ECPA does not apply to several modern monitoring techniques, such as electronic mail monitoring and video surveillance [1, p. 841].

Pennsylvania contains a wiretapping statute similar to the ECPA. However, Pennsylvania's Wiretapping and Electronic Surveillance Act is a criminal statute, and courts have recognized that it should be narrowly construed because it is designed to regulate surreptitious electronic monitoring of citizens by the government officials. However, the courts have also found that private individuals may be prosecuted for violating the Wiretap Act's provisions.

COMMON LAW PROTECTION

Under common law, a person's privacy may be invaded by an unreasonable intrusion upon his/her seclusion. Most plaintiffs use this tort to challenge employer monitoring and surveillance [1, pp. 825, 844]. The tort reads in part: "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person" [23]. The classic conception of this tort is that it is used to punish highly offensive privacy invasions [1, pp. 825, 844]. Recognized in virtually every state, there has been an attempt to apply the tort in the employment context as a way of challenging workplace-monitoring abuses by employers [1, pp. 825, 844; 24, §3.3, p. 108; §3.5, p. 123]. However, what is "highly offensive to a reasonable person" is a very subjective standard. Routine monitoring may appear harmless from some perspectives (especially that of a third party), and the negative effects of such monitoring may be gradual and incremental, so this subjective standard usually defeats an employee's claim based on typical workplace monitoring and surveillance [1, p. 845].

In *Smyth v. Pillsbury Co.,* an employee was terminated after his employer intercepted an e-mail message from the employee to his supervisor via the employer's e-mail system and determined the e-mail contained "inappropriate and unprofessional comments" [17, pp. 695, 743; citing 25]. The employee sued for wrongful termination, claiming his termination violated the right to privacy "as embodied in Pennsylvania common law [17, p. 743; citing 25, at 100]. The court noted that although the plaintiff was an at-will employee who could generally be terminated with or without cause, no employee could be terminated if the discharge threatened or violated a "clear mandate of public policy" [17, p. 743; citing 25, at 99]. The court concluded, however, that the plaintiff's termination did not violate public policy [25].

The court began its analysis by holding there could be no "reasonable expectation of privacy" in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system [17, p. 743; citing 25, at 101]. The court also made clear it would reach the same conclusion even if an employer gives assurance that such communications would not be intercepted [17, p. 743; citing 25]. The court then stated that, even if an employee had a reasonable expectation of privacy in electronic communications, interception by an employer would not constitute "a substantial and highly offensive" invasion of privacy. The court concluded that an employer's interest in preventing inappropriate or illegal conduct outweighs any privacy interest an employee might have in his e-mail communications [17, p. 743; citing 25, at 101].

As this case demonstrates, courts have not been very receptive to employee claims of invasion of privacy. An employee's office, desk, or locker may be held to be the employer's property, and thus not private [1, pp. 825, 846]. Moreover, some

courts require an employee to demonstrate not only the occurrence of an invasion of privacy, but also that the employer subsequently disseminated or published the information obtained from that intrusion [1, p. 846]. The combination of these requirements typically defeats the employee's tort claim in all but the most egregious circumstances [1, p. 846; 26].

PROPOSED PRIVACY PROTECTIONS

Though many commentators have questioned the lack of workplace privacy protection for nongovernment employees, no consensus has emerged as to a solution to the problem [1, p. 847]. Recommendations include suggestions of new state laws or tort actions, amending current federal privacy protection statutes, and even Constitutional amendment.

In 1993, the Privacy for Consumers and Workers Act (PCWA) was introduced in the U.S. House of Representatives and the U.S. Senate. In February 1994, the House Education and Labor Subcommittee on Labor Relations approved the bill. However, the PCWA met with strong resistance in the Republican committee and thus remained inactive. [At press time, in 2001, the bill was still in committee.]

Generally, the PCWA would require employers to give specific written notice to their employees concerning: 1) the forms of monitoring to be used; 2) the use (if any) to be made of personal data collected; 3) interpretations of statistics or other records if the interpretations affect the employee; 4) existing production standards and work performance expectations; and 5) methods for determining production standards and work performance expectations based on electronic monitoring statistics [17, p. 737]. The PCWA would also require notice to job applicants and customers who may be electronically monitored pursuant to the PCWA [17, p. 737].

Under the PCWA, an employer could monitor any employee at the worksite without notice if the employer "has a reasonable suspicion" that the employee has violated or will violate criminal law or civil law, or has engaged in or will engage in gross misconduct and the conduct adversely affects the employer's economic or safety interests. The proposed PCWA does not delineate what types of monitoring may be inappropriate even with adequate notice, leaves employees subject to offensive nonelectronic monitoring, and fails to protect the employee against egregious privacy violations that meet the notice requirements [1, pp. 825, 851].

Although the PCWA may have its shortcomings, it is a major step toward adequate privacy protection for the employee in the private sector workplace.

Other scholars have suggested an expansion of the privacy tort to help deter workplace privacy invasions. Supporters of an expanded privacy tort argue that a new common-law cause of action applying to all workplace privacy invasions would provide the greatest protection to employees [1, pp. 825, 851]. Supporters theorize that the courts can fashion new common-law remedies to resolve the problems created by changes in technology and economic conditions. Because

legislation has not dealt adequately with these issues, supporters believe a new tort claim would provide the most immediate help to workers. The tort law approach of adjudicating claims on a case-by-case basis, examining the circumstances and balancing the equities of each case, would provide the best mechanism for protecting privacy rights [1, p. 852]. However, a judiciary expansion of current privacy doctrine would involve broadened rulings, which the courts seem unwilling to make. In addition, action by the courts would not provide uniform protection of workplace privacy rights. Employees who suffer similar intrusions might receive differing protection of their privacy rights, and the surveillance process may cross state lines [1, p. 853]. As a result, employees and employers may be uncertain as to which law governs their workplace rights.

CONCLUSION

Despite our historic commitment to privacy rights in the United States, it has become increasingly common for employers to monitor the actions and communications of their employees [1, p. 887]. As advances in technology are made, electronic monitoring in the workplace may well become even more prevalent. Abuses of these practices are bound to become more commonplace unless some guidelines are established. At present, Congress and state legislatures have recognized some limitations on the employer's ability to monitor employees [1, p. 887]. Current privacy law, however, is inadequate and inconsistent [1, p. 887]. The best solution would be to adopt a comprehensive federal statute based on broad constitutional principles of privacy. This seems to be the only way to address the lack of privacy protection that currently exists for private sector employees, while at the same time providing a uniform statute that would not vary from state to state and from jurisdiction to jurisdiction.

In addition to the need for legislative action, a balance must be struck between the employer's need for monitoring employee performance and the employee's legitimate privacy and productivity interests. Courts need to examine more closely the claims of business necessity for privacy intrusions and should recognize that less intrusive methods of determining employee productivity can achieve similar results. Employers must also recognize that electronic monitoring may not achieve the benefits they anticipate, since studies have indicated that electronic monitoring may lower work performance and productivity. Finally, employees must also recognize and accept some level of monitoring, for if employees demand the complete elimination of electronic surveillance, employers may invade employee's personal integrity through even more degrading means than those now occurring.

* * *

Paul Kovatch received his B.S. in Accounting from Wilkes University in 1993. He received his J.D. from the Widener University School of Law at Harrisburg, Pennsylvania.

ENDNOTES

1. Elizabeth Wilborn, Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace, 32 *Georgia Law Review,* pp. 825-887 (1998), citing Rosemary Orthmann, *Most Major Employers Monitor Workers Electronically,* American Management Association International Survey Questionnaire: Workplace Testing and Monitoring, University Publications of America, Bethesda, Md. (May 1997). The survey indicated 63 percent of its members conducted electronic monitoring or surveillance of employees.
2. Andrew Jay McClurg, Bringing Privacy Law Out of the Closet: Tort Theory of Liability for Invasions in Public Places, 73 *North Carolina Law Review,* pp. 989-1089, 1017 (1995). Noted startling increase in monitoring of employees and customers.
3. [No author cited], Addressing the New Hazards of the High Technology Workplace, 104 *Harvard Law Review,* pp. 1898-1916, 1903 (1991). Noted that employers can record length, time, and destination of calls with computerized telephone system technology.
4. U.S. Congress, Office of Technology Assessment, *The Electronic Supervisor: New Technology, New Tensions* (OTA-CIT-333), Washington, D.C.: U.S. Government Printing Office, September 1987. Described possible illegitimate uses of monitoring, such as frustration of union organizing efforts, circumvention of employment discrimination laws via intensified scrutiny of protected employees, and identification of whistleblowers.
5. *Harris v. Neff,* 55 Fair Employment Practices Cases, BNA 1019; 6 IER Cases 615 (D. Kan., March 25, 1991. [Not reported in Federal Supplement.] Finding: A memorandum circulated to 110 employees was not considered highly offensive to a reasonable person and did not constitute privacy invasion. The memorandum had stated that a worker was no longer employed and had voluntarily entered an alcohol and drug rehabilitation program.
6. Raymond Wacks, *The Protection of Privacy* (London: Sweet & Maxwell Publishing, 1980). The author noted: "The long search for a definition of 'privacy' . . . is often sterile and, ultimately, futile" [p. 10].
7. Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967). The author stated: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, and to what extent, information about them is communicated to others" [p. 7].
8. *Roe v. Wade,* 410 U.S. 133 (1973).
9. *Board of Regents of State Colleges v. Roth,* 408 U.S. 564 (1972).
10. Ken Gormley, One Hundred Years of Privacy, *Wisconsin Law Review,* pp. 1335-1441 (1992).
11. Gormley described how "the industrialization and urbanization of America in the late 1800s . . . threatened the ability of individuals to regulate . . . information concerning themselves, an essential function if they were to help mold the perceptions society would form of them, the essence of individuality" [10, p. 1434].
12. Gormley noted that fundamental-decision privacy, such as whether to have an abortion and how to raise one's family, has links to equality [10, pp. 1434-1438].
13. *Gay Law Students Association v. Pacific Telephone & Telegraph Company,* 595 P.2d 592, 599 (Cal. 1979). The ruling included: "An individual's freedom . . . to work and

earn a living has long been recognized as one of the fundamental and most cherished liberties enjoyed by members of our society. . . ." [at 599].

14. Julie A. Flanagan, Restricting Electronic Monitoring in the Private Workplace, 43 *Duke Law Journal,* pp. 1256-1281, 1262 (1994).
15. David Neil King, Privacy Issues in the Private Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap," *Southern California Law Review,* pp. 441-474 (1994).
16. *O'Connor v. Ortega,* 480 U.S. 709 (1987).
17. Thomas P. Klein, *Electronic Communications in the Workplace: Legal Issues and Policies,* Handbook: 563 (New York: Practicing Law Institute/Pat., 1999), pp. 695-754.
18. *Commonwealth v. Parker,* 422 Pa.Super. 393 (1993).
19. Omnibus Crime Control and Safe Streets Act, Public Law No. 90-351, 82 Stat. 197, 211-225 (1968).
20. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510(5)(a). The act exempts interceptions occurring "in the ordinary course of . . . business" from the definition of interceptions.
21. *Briggs v. American Air Filter Co., Inc.,* 630 F.2d 414 (1980). The court found the defendant employer had acted in the ordinary course of business when it monitored an employee's telephone calls to a competitor who was also a friend of the employee as well as a former employee of the defendant. According to the court, the employer had reason to suspect its employee was discussing confidential information with former employee.
22. Larry O. Gantt, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 *Harvard Journal of Law and Technology,* pp. 345-425 (1995).
23. Restatement (Second) of Torts, § 625B (1977).
24. Kurt H. Decker, *Employer Privacy Law and Practice* (Amityville, N.Y.: Baywood Publishers, 1987; *Supplement,* 1997). The author discussed the lack of remedies available to most private sector workers for invasion-of-privacy claims.
25. *Smyth v. Pillsbury Co.,* 914 F. Supp. 97 (E.D. Pa. 1996).
26. *Doe v. B.P.S. Guard Services, Inc.,* 945 F2d 1422, 1427 (8th Cir. 1991). The court held the security-guard firm liable for the invasion of privacy that occurred when guards videotaped models changing clothes in the dressing area at a fashion show.

Direct reprint requests to:

Paul Kovatch
6130 Springford Drive
Apt. K6
Harrisburg, PA 17111