Privacy in the Workplace

Kevin J. Conlon
PRIVACY IN THE WORKPLACE

KEVIN J. CONLON*

INTRODUCTION

The rapid growth of workplace monitoring and surveillance technology has far outpaced the development of laws that protect worker privacy interests. While the monitoring of workers is hardly a new phenomenon, modern technology has provided employers with more advanced and effective means of monitoring their employees. As a result, electronic monitoring of employees in the workplace has become far more prevalent in recent years. Not only are employers collecting more data on their employees,¹ they are collecting more kinds of data. Technology now enables an employer to record every keystroke on the computer, every syllable uttered to a customer, and every second spent away from one's work station. These enhanced monitoring capabilities do not come without a price: they come at the expense of employee privacy and health. Further, they do not yield the benefits promised. Studies indicate that pervasive electronic monitoring in the workplace actually reduces worker productivity.²

As Professor Finkin correctly points out, our current legal system is inadequate to deal with these issues.³ Constitutional protections do not extend into the workplace, exceptions to statutory limitations ex-

* Kevin J. Conlon is an attorney in private practice and serves as District Counsel for the Communications Workers of America. He is a frequent lecturer and author on labor law subjects.

1. According to Morton Bahr, president of the Communications Workers of America, private employers are expanding the practice of electronically monitoring their employees. In his testimony before the Subcommittee on Employment Productivity, he reported that the number of monitoring systems sold to businesses soared by nearly 200% between 1985 and 1988 and that sales have continued to rise. The Privacy for Consumers and Workers Act, 1991: Hearings on S. 516 Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor and Human Resources, 102d Cong., 15 (1991) (statement of Morton Bahr, President, Communications Workers of America) [hereinafter CWA Testimony].

2. According to a report prepared for the U.S. Office of Technology Assessment, there is currently no research evidence which demonstrates that electronic monitoring actually increases individual worker production levels. See generally MICHAEL J. SMITH, PH.D., ET. AL., MOTIVATIONAL, BEHAVIORAL AND PSYCHOLOGICAL IMPLICATIONS OF ELECTRONIC MONITORING OF WORKER PERFORMANCE (1986) (Prepared for the Office of Technology Assessment, United States Congress) [hereinafter WORKER PERFORMANCE STUDY]. To the contrary, in many cases the negative effects of electronic monitoring (e.g., increased employee stress) have actually resulted in a sharp decrease in employee productivity. See id.

empt most employer monitoring, and the common law legitimizes otherwise intrusive behavior if an employer can demonstrate a business purpose. This Article first briefly outlines the law of privacy in the workplace and then discusses some of the key issues posed by electronic monitoring in that setting.

I. SUMMARY OF THE LAW

A. Federal Constitution

While the Constitution does not specifically recognize the right to privacy, the Supreme Court has identified certain zones of privacy in which government action is limited. These zones of privacy only protect against intrusive state action. The Court has been reluctant to find state action in the private sector, and consequently, private sector employees must look to statutory, case, and contract law for protection from intrusive employers.

B. State Constitutions

Several states have incorporated specific privacy guarantees into their constitutions. With the exception of California, these constitutional provisions do not extend to employees in the private sector. In California, the courts have held that the state constitution prohibits all intrusions into an individual’s private matters unless the employer can show a “compelling interest” that justifies the invasion. The “compelling interest” test has been applied to situations involving drug

4. See Griswold v. Connecticut, 381 U.S. 479 (1965) (The Griswold Court held that a Connecticut statute restricting the use of contraceptives by married couples was unconstitutional on the ground that it impinged on matters “concern[ing] a relationship lying within the zone of privacy created by several fundamental constitutional guarantees.” Id. at 485. The Court based its decision on the First, Third, Fourth, Fifth, and Ninth Amendments. See id. at 484.); see also, Roe v. Wade, 410 U.S. 113, (1973) (The Court recognized an individual’s general right to hold certain private matters away from public scrutiny. In Roe, the Court enumerated those areas of personal autonomy which deserve constitutional protection and subsequent courts have strictly limited the right to privacy to these enumerated categories.).


7. See, e.g., Bianco v. American Broad. Co., 470 F. Supp. 182, 186-87 (N.D. Ill. 1979) (The right to be secure against “unreasonable ... invasions of privacy or interceptions of communications by eavesdropping devices or other means” as set forth in Article I, Section 6 of the Illinois Constitution, is a limitation on governmental activity only.).

screening and psychological testing with favorable results. California's constitutional right to privacy has not been examined in the context of electronic surveillance of employees, however, and it is unlikely that the "compelling interest" test will provide much protection from overly intrusive employer supervision. Employers will undoubtedly assert a vast number of business purposes that will legitimize their use of service quality observation technology, computerized work-measurement devices, and video surveillance equipment. The California courts will most likely find those purposes "compelling" under the constitution. Thus, state constitution privacy clauses are no more protective of worker privacy interests than the federal Constitution.

C. Federal Statutes

The Electronic Communications Privacy Act of 1986 ("ECPA") protects against the interception, disclosure, and intentional use of wire and electronic communications by both private and public parties absent prior judicial authorization. The statute's protections apply only if the interception is accomplished through the use of an "electronic, mechanical or other device." Thus, an employer can listen to an employee's conversation on an extension telephone without violating the statute.

The statute contains two sweeping exceptions relevant to the workplace setting. The first is the prior consent exception which provides that the interception of oral, wire, or electronic communications shall not be unlawful if one of the parties to the conversation has given prior consent to the interception. The "prior consent" exception has been interpreted narrowly in the employment context: consent will rarely be implied and cannot be given on behalf of the

9. See Luck v. Southern Pacific Transportation Co., 267 Cal. Rptr. 618 (1990) (upholding the claim of a computer programmer who refused to take a urine test in a wrongful discharge case); see also, Soroka v. Dayton-Hudson Corp., 1 Cal. Rptr. 2d 77 (1991) (The appellate court reversed the lower court and held that the employer's interest in securing psychologically fit applicants for important security positions was not compelling enough to justify asking highly intrusive questions about the applicants' religion and sexual preferences on a job application.).
12. See Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (finding that "[i]t is in the ordinary course of business to listen in on an extension phone for at least as long as the call involves the type of information he fears is being disclosed").
14. See Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (consent could not be implied from the circumstances because no reasonable person would have consented to the taping of conversations about their participation in a theft or their sexual activities); Watkins v. L.M.
employee by the employer. Generally speaking, however, consent is expressly given in employment contracts as a condition of employment.

The second major exception to the statute's protection is the "business use exception." The business use exception effectively legalizes most workplace telephone monitoring by employers. The test is whether the interception was made "in the ordinary course of business." In applying the test, courts have focused on the equipment used and the circumstances under which the monitoring took place. Few limits have been placed on the type of equipment that can be used and the courts have broadly interpreted the circumstances that are considered to be "in the ordinary course of business." Employers can monitor the phone lines to assure adequate customer service, prevent unauthorized use of the phone lines, or prevent disclosure of confidential information. Employers are limited in their ability to intercept personal conversations, however, and they can listen only long enough to determine that the conversation is personal in nature. Thus, the ECPA provides very little protection to the employee in the workplace.

Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (knowledge of the capability of monitoring alone cannot be considered implied consent).

15. The language and legislative history of § 2511(2)(d) make it clear that consent can only be given by one of the parties to the communication. See S. Rep. No. 90-1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2182 (citing United States v. Pasha, 332 F.2d 193 (7th Cir. 1964)).


17. Id.

18. See, e.g., Deal, 980 F.2d at 1157 (finding that an automatic tape recorder that is not connected to the phone line does not fall under the exception).


20. See Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (finding that an actual consent to a policy of monitoring sales calls was not consent to the monitoring of private calls except to the extent necessary to determine their nature).

21. See Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (The court found that the employer had acted in the ordinary course of business when it monitored employee phone calls made to a competitor. The following facts influenced the court's decision: (1) the plaintiff admitted that the call was of a business, rather than a personal nature; (2) the supervisor's act of surveillance was limited in purpose and time; and (3) the surveillance was not part of a general practice of secret monitoring.).

22. See Watkins, 704 F.2d at 584 (permitting an employer to listen to a personal call for a time sufficient to determine the call's nature, but no longer).
D. State Statutes

Most states have enacted legislation prohibiting electronic monitoring and surveillance by private individuals.23 The statutes generally mirror their federal counterpart and include the prior consent and business use exceptions.24 In a handful of states, both parties to the conversation must consent to the interception.25 In all states, consent can be express or implied.

In at least one state, the legislature amended the state anti-eavesdropping statute to allow more general telephone monitoring of employees.26 The statute would have permitted monitoring "for educational, training or research purposes."27 The statute so worded would have given employers the right to monitor almost any phone call for almost any reason. Fear of abuse prompted unions in the state to campaign against the statute. The legislature responded by amending the statute and limiting its applicability to "quality control of marketing or opinion research or telephone solicitation."28 From the employee's perspective, state anti-eavesdropping statutes provide very limited protection from overly intrusive monitoring practices.

E. Common Law

Since constitutional and statutory law provide limited privacy protection to individuals at work, the discussion of worker privacy rights has largely focused on common law privacy claims. The common law of privacy is comprised of four distinct causes of action: (1) unreasonable intrusion into seclusion; (2) public disclosure of embar-


25. California, Delaware, Florida, Georgia, Illinois, Maryland, Massachusetts, Michigan, Montana, New Hampshire, Pennsylvania, and Washington all require both parties' consent to the monitoring. See CAL. PENAL CODE §§ 631(a), 632(a) (West 1996); DEL. CODE ANN. tit. 11, § 1336(b) (1995); Fla. Stat. ch. 934.03(2)(d) (1995); GA. CODE ANN. § 16-11-66(a) (1996); 720 ILL. COMP. STAT. 5/14-2 (West 1993); MD. CODE ANN., Cts. & Jud. Proc. § 10-402(c)(3) (1995); MASS. GEN. LAWS ANN. ch. 272 § 99(B)(4) (West 1990); MICH. COMP. LAWS ANN. § 750.539c (West 1991); MONT. CODE ANN. § 45-8-213(c) (1995); N.H. REV. STAT. ANN. § 570-A.2 (1986); 18 PA. CONS. STAT. ANN. §§ 5703-04 (West 1995); WASH. REV. CODE ANN. § 9.73.030(1)(b) (West 1988). Note, however, that many state courts have interpreted these statutory provisions to only require one party's consent to the monitoring, despite the explicit statutory language to the contrary. See e.g., People v. Beardsley, 503 N.E.2d 346, 350 (Ill. App. Ct. 1986) (interpreting the Illinois statute to require the consent of only one of the parties to the conversation).


27. Id.

rassing private facts; (3) public portrayal of an individual in a false light; and (4) appropriation of another person's name or likeness. This Section will focus on the first of these causes of action: intrusion into seclusion.

An intrusion case requires a prima facie showing of three elements: (1) an intrusion; (2) into a private matter; (3) that is highly offensive to a reasonable person. Intrusion claims are largely determined by the third element: the employee's reasonable expectation of privacy and the offensiveness of the intrusion. In practice, courts will first define the scope of an employee's reasonable expectation of privacy and then balance the employer's business interest against the employee's individual rights.

In the workplace setting, the employer defines an employee's reasonable expectations of privacy by establishing office policy and procedure. Given the large number of legitimate business interests that can be advanced through the use of electronic monitoring devices, it is often difficult for an employee to establish a reasonable expectation of privacy. Further, because electronic surveillance technologies are designed to be physically nonintrusive, employees have had difficulty proving the highly offensive nature of electronic monitoring techniques. In practice, the common law intrusion into seclusion claim provides only limited protection for worker privacy interests.

30. THE RESTATEMENT OF TORTS § 652B (1977), defines the tort of intrusion upon seclusion as: "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."
31. See id.
32. See, e.g., Johnson v. Corporate Special Services, Inc., 602 So.2d 385, 386 (Ala. 1992) (The court based its decision on whether the plaintiff should have anticipated an investigation into his physical well-being after filing a worker's compensation claim.); Alabama Electric Co-Operative v. Partridge, 225 So.2d 848, 851 (Ala. 1969) (finding that the plaintiff had a reduced expectation of privacy after filing a personal injury claim and then balances that interest against the employer's business interest in not paying a fraudulent personal injury claim).
33. Courts grant a great deal of deference to employer business interests, making it clear that employees are not entitled to the same degree of privacy at work that they enjoy at home. Employer interests play a clear role in defining what is "reasonable." Generally speaking, so long as the monitoring is limited to job performance or related matters, courts will find that the monitoring activity was not "highly offensive to a reasonable person." Some courts have even read employer business interests to allow off-site monitoring of workers. See, e.g., Johnson v. Corporate Special Services, Inc., 602 So.2d 385, 388 (Ala. 1992) (The court held that an employer's off-site surveillance of an employee who had filed a worker's compensation claim against the employer did not violate the employee's privacy. The employer was found to have a legitimate interest in determining the scope of the employee's injuries.).
34. Some would argue that electronic monitoring techniques are less intrusive than traditional monitoring techniques. For example, a hidden camera is less obtrusive than direct oversight by a supervisor. This argument, however, fails to recognize the pervasive and constant
II. Analysis

Currently, an employer's right to engage in service quality observation, computerized work measurement, and video surveillance of employees is relatively unrestricted. The employee enjoys a very narrow zone of privacy in the workplace. Professor Finkin correctly argues that the zone is too narrow. Professor Westin disagrees and contends that while the use of electronic monitoring devices may pose problems in the areas of fair work standards, employee dignity, and employee health, privacy is not at issue. He feels that privacy-based attacks on electronic monitoring in the workplace are invalid, and argues that they "lack[ ] public support, threaten[ ] societal interests in quality work, and fundamentally misappl[y] privacy concepts."\(^{35}\) The balance of this Section will address these claims.

A. Public Support for Fair Employer Monitoring

After a careful examination of public opinion surveys on privacy in the workplace, Professor Westin concludes that our legal system accurately reflects the general public perception of what constitutes reasonable and unreasonable expectations of privacy at work. He writes: "On the whole, what we have written into law and judicial decision, and what has not been put into law in the various areas of workplace privacy is a solid, workable system that strikes the right balances between privacy and other social interests."\(^{36}\)

There are several problems with this conclusion. First, as Professor Finkin explains, employees are largely unaware of the scope and amount of electronic monitoring that actually takes place. According to Morton Bahr, president of the Communications Workers of America, companies spy on as many as 400 million telephone calls each year.\(^{37}\) A MacWorld survey revealed that 20 million Americans may be subject to monitoring through their computers, and an estimated 375,000 have had their e-mail files searched. Fewer than one-third of employees utilizing electronic monitoring devices warn their employees that such methods are in use.\(^{38}\) These numbers are cause for concern. The fact that ninety percent of all employees believe that


\(^{36}\) Id. at 283.

\(^{37}\) See CWA Testimony, supra note 1 at 15.

\(^{38}\) Charles Piller, Bosses With X-Ray Eyes, MACWORLD, July 1993, at 123.
their employer has never sought inappropriate personal information indicates a lack of understanding of the pervasiveness of employer monitoring, not a general satisfaction with current legal protections for worker privacy interests.

A separate issue brought out in Westin's analysis is the problem of notice. According to Westin, over ninety-three percent of the employees surveyed feel that "[p]rocedures for listening-in and standards used to evaluate employee call-handling should be fully explained to employees."\(^{39}\) Recall that fewer than one-third of employers actually warn employees that electronic surveillance is in use. The obvious question, then, is whether knowing about the absence of notice would have diminished the survey participants' overall satisfaction with current legal protections for worker privacy interests. Given how highly the survey participants seem to value notice, the answer is most likely "yes."

A final issue, touched upon in Westin's argument is the problem of consent. Ninety-two percent of the respondents in Westin's survey felt that "[e]mployees should be told when they are hired for these jobs that supervisors will sometimes listen-in on business calls, so that employees can agree or not agree to work under these procedures."\(^{40}\) This response indicates that the survey participants place a high value on the opportunity to consent to monitoring. It is important to note that the survey question fails to indicate that consent to monitoring is almost always given under duress; employers generally require potential employees to consent to electronic monitoring as a pre-condition to employment. This begs the question: Would the participants in Westin's survey have been as comfortable with employee monitoring techniques had they realized that consent to monitoring was not given voluntarily? Clearly, the participants in Westin's survey were not given enough information about actual electronic monitoring practices to respond knowledgeably on the subject.

B. The Threat to Central Societal Interests in Quality Work

Professor Westin contends that privacy-based arguments against the use of intrusive electronic monitoring devices pose a threat to "central societal interests in quality work."\(^{41}\) In making this argument, Westin necessarily assumes that the electronic monitoring of

\(^{39}\) Westin, supra note 34, at 281 (emphasis added).

\(^{40}\) Id. (emphasis added).

\(^{41}\) Id. at 278.
workers results in enhanced work quality. There is strong evidence that the opposite is true. Studies have shown that the adversarial atmosphere created by monitoring undermines employee self-esteem and dignity, which decreases job commitment and results in lower productivity and competitiveness. In addition to the productivity cost, monitoring adversely affects customer service by overemphasizing quantity of work at the expense of quality. The following anecdote illustrates this point: A telephone operator generally handles 1100 calls in a 7.5 hour shift. The operator must complete each call in twenty seconds or less, and the time in which it takes to complete the call is monitored. If she fails to meet the time limit, she can be dismissed. A Catch-22 situation arises when she receives a call from a customer with a speech impediment, hearing problem, learning handicap, or language barrier. She must choose between preserving her job and providing quality customer service. In one case, an operator received a call from a customer who stated he was considering suicide. The operator’s manager willfully disconnected the call after fifteen minutes because the operator was taking too long to complete the call. Clearly the real threat to work quality is not privacy-based opposition to electronic monitoring in the workplace; it is the misuse of electronic monitoring devices in the workplace.

C. Fundamental Misapplication of Privacy Concepts

Professor Westin charges that privacy-based objections to electronic monitoring in the workplace are really disguised protests against worker supervision. Such objections, he argues, “stretch[ ] the concept of privacy beyond its rational limits.” Privacy, in his mind, is a concept that has been exploited as “an emotionally-charged weapon in the on-going power struggle between management and unions.”

In making these statements, Westin fails to recognize an important feature of electronic monitoring: its pervasive nature and the impact that such has on worker privacy interests. Consequently, he does not acknowledge that a system of total oversight intrudes upon worker privacy interests because of its constant presence. The follow-

42. See Worker Performance Study, supra note 2, at 16-21.
43. See CWA Testimony, supra note 1, at 18.
44. See id.
45. See id. at 19.
46. See CWA Testimony, supra note 1, at 19.
47. See id.
49. Id. at 277.
ing quote from an telephone operator illustrates the degrading impact of electronic monitoring in the workplace:

In our office, they turn on the blue light . . . that is only supposed to be on when someone is monitoring, but most days it is turned on at 8 a.m. and stays on all day. We did have three supervisors that do nothing but monitor us all day. We now have a new supervisor in our department, and they have put her on monitoring also.

I have been with Bell Company 29 years. [This] is the worst department I have been in all my years with the company.

They use monitoring to see if they can find something to charge against you. I find it to be dehumanizing, unhealthy and disgusting.

Through the years I have been appraised as more than satisfactory and respected to do work without constant supervision.

All in our department feel as though we are in prison and we are regarded as nothing more than criminals that must be guarded and monitored on constantly as though we could not function on our own. We are all adults, but we are made to feel like naughty children.

I loved my job I had before. Now all I long for is the day I can retire and never have to set foot back in that horrible place.  

When every second at work is spent under the watchful, unblinking eye of an electronic monitoring device, can a worker really be said to have any privacy rights in the workplace? Professor Finkin would argue no. Constant and pervasive electronic monitoring effectively eliminates the narrow zone of privacy that workers are accorded under the law. Because our legal system fails to address the effects of a program of total and constant worker oversight, Finkin argues persuasively for reform.

III. Reforming the System

Thus far this Article has focused upon the inadequate protection afforded by our current legal system to worker privacy interests. It is clear that legal reform is necessary to guarantee that individual privacy interests are protected from overly intrusive electronic monitoring devices. Because tort reform is a slow and unwieldy process, change must come from the legislature. What follows is a list of the reforms needed to protect individual privacy interests in the workplace:

50. CWA Testimony, supra note 1, at 19.
PRIVACY IN THE WORKPLACE

(1) There should be no monitoring in highly private areas such as restrooms, locker rooms, and employee lounges. Time spent away from one’s work station can be monitored in less invasive and less offensive ways.

(2) Monitoring should be limited to the workplace, and any offsite monitoring should be prohibited. An employee should not have to sacrifice his or her right to privacy outside the workplace merely because he or she agreed to work for an employer.

(3) Employees should have full access to any and all information gathered through monitoring techniques. They should also be given the right to refute or appeal the validity of that information in a timely fashion.

(4) Continuous monitoring should be banned. Electronic employee observation should be limited to a maximum of two hours each day.

(5) All forms of secret monitoring should be banned. Employees should be given advance notice of the devices that will be used to monitor their work, how that data will be used, and the exact time and date that monitoring will take place.

(6) Employees and customers should be put on notice when telephonic monitoring is taking place through the use of a “beep” tone, audible to both employee and consumer.

(7) Employers should be limited in the information that they can gather: only information relevant to that job should be collected.

(8) Monitoring must result in the attainment of some business interest. It should not be enough to claim that monitoring increases productivity or quality of performance: the employer should be required to demonstrate that the goal is met.

Conclusion

With the change in emphasis in our economy from manufacturing to service, the workplace has been transformed into an electronic office. At the same time, the means by which management seeks to monitor and control workers has undergone a dramatic change. Visual observation and daily production counts have been replaced by
electronic monitoring devices. Secret monitoring devices have literally brought “Big Brother” into the office. Proponents of legislative reform of workplace privacy laws believe that “the use of bugging devices, employee monitoring computers and video cameras has turned jobsites into detention centers where the rights of privacy are surrendered at the door.” The law has been slow to react to the insurgence of monitoring technology in the workplace and employers have been faced with relatively few legal restrictions on their use of this technology. Professor Westin would argue that our legal system has struck the correct balance between worker privacy interests and employer business interests. The reality is, however, that the legal protection of employee privacy interests has lagged far behind the promotion of employer business interests. As we move towards the twenty-first century, it is clear that electronic monitoring devices will play a major role in the workplace. It is therefore essential that the evolution of electronic monitoring technology be mirrored by the development of laws designed to protect the privacy interests of workers.

51. “DON’T BUG ME:” CONSUMER AND WORKER ACTION KIT TO PROTECT WORKPLACE PRIVACY 4 (prepared by the Communications Workers of America).
STUDENT NOTES AND COMMENTS