Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise form the Modern Sweatshop

Robert G. Boehmer

Follow this and additional works at: https://via.library.depaul.edu/law-review

Recommended Citation
Available at: https://via.library.depaul.edu/law-review/vol41/iss3/5
ARTIFICIAL MONITORING AND SURVEILLANCE OF EMPLOYEES: THE FINE LINE DIVIDING THE PRUDENTLY MANAGED ENTERPRISE FROM THE MODERN SWEATSHOP

Robert G. Boehmer*

I. INTRODUCTION

The vast arsenal of technology now available to employers for the day-to-day gathering and analysis of information about their employees is impressive, as well as frightening. Except for outrageous conduct and the use of one of a discrete group of techniques that Congress has chosen to regulate, the law supplies employees with precious little protection from the assault on workplace privacy. Similarly, the law provides employers with little guidance concerning the permissible depth of their intrusions. Legislation designed to plug this gap in workplace privacy law is now pending before both the United States Senate and House of Representatives. The primary purpose of this

---

* Assistant Professor of Legal Studies, Terry College of Business, University of Georgia. B.S. (Business Administration), University of Oregon (1974); J.D., University of Oregon (1977). The author is a member of the Oregon State Bar.

1. S. 516, 102d Cong., 1st Sess. (1991) [hereinafter Senate Bill]. This bill was introduced on February 27, 1991, by Senator Paul Simon. 137 CONG. REC. S2430 (daily ed. Feb. 27, 1991). Senator Simon, in introducing this bill, stated that "[i]t is an unfortunate irony that the Federal Bureau of Investigation is required to obtain a court order to wiretap a telephone, even in cases of national security, but that employers are permitted to spy at will on their own personnel and the public." Id. The bill was referred to the Senate Labor and Human Resources Committee on February 27, 1991. 137 CONG. REC. S2404 (daily ed. Feb. 27, 1991). Hearings were held on the bill on September 24, 1991, before the Subcommittee on Employment and Productivity. 137 CONG. REC. D1137 (daily ed. Sept. 24, 1991). The bill, originally sponsored by Senator Simon, is now co-sponsored by Senator Paul Wellstone. A similar proposal was introduced by Senator Simon the prior year, S. 2164, 101st Cong., 2d Sess. (1990), but died in committee. A recent report describes the likelihood of passage as "far from a sure thing." Louise Fickel, Don't Look Now, But . . . .: A New Crop of Network Products Is Forcing a Debate Over Workplace Monitoring, INFOWORLD, May 13, 1991, at 50, 54; see also John P. Furfaro & Maury B. Josephson, Electronic Monitoring in the Workplace, N.Y. L.J., July 6, 1990, at 3 n.3 (discussing prior legislative proposals concerning this subject matter by Senator Simon).


739
Article is to make a small contribution to the debate concerning those legislative proposals.

The legislation pending before Congress is certainly not a panacea for the problem. For example, some workplace privacy concerns, such as worries about genetic testing, must remain beyond the scope of legislation at this time. In addition, increased flexibility is needed in certain aspects of pending legislative proposals. However, those proposals represent an important first step towards a long-term solution.

A thorough analysis of each of the many technological devices available to employers and the patchwork quilt of laws regulating the use of those devices is beyond the scope of this Article. However, the need for federal legislation cannot be communicated without some understanding of the current technology in the American workplace and the laws that now regulate it. This understanding of technology and law reveals the delicate nature of the balance

---

3. See infra part V (discussing inadequacies of legislative proposals pending before Congress).
4. See infra part II.C (discussing the wide array of technologies available for employee monitoring and surveillance).
5. See infra part III (reviewing the patchwork quilt of statutory and common law remedies available to employees for employer intrusions into the employee's privacy).
that must be struck by Congress. As stated in a recent report on workplace privacy, "Reconciling the need for increased information about employees with expanding privacy rights is a problem of increasing importance in managing the changing work force of the 1990s."  

In addressing this delicate balance, this Article first presents an overview of the current state of artificial monitoring and surveillance in the American workplace. The Article discusses competing employer and employee interests, available technology, the extent of the current use of that technology, the distinction between that technology and human supervision, and the resulting impact of technology on employees. Next, the Article presents an overview of the existing regulatory maze governing artificial monitoring and surveillance of employees in the private sector. To illustrate the inadequacy of the existing legal structure, the Article examines federal and state law on eavesdropping upon employee telephone calls and shows how an exception to the prohibition on unauthorized "listening" virtually can swallow the rule. Other federal and state limitations, such as those placed on polygraph examinations, are presented in summary fashion in order to illustrate the myriad and inconsistent laws affecting artificial monitoring and surveillance of employees, none of which effectively and fairly regulates it.

In conjunction with this overview of the law, the Article examines the adequacy of these existing legal limitations in light of the rapidly expanding role of artificial monitoring and surveillance in the American workplace. Technological advances have occurred simultaneously with major changes in the nature of the workplace. These changes include the erosion of the employment-at-will doctrine, the decreasing unionized segment of the workforce, and increasing demands for productivity, caused in part by competitive demands resulting from international competition.

The Article then addresses the central question: Do these changes in technology and in the workplace warrant the enactment of a federal statute designed to appropriately balance legitimate employer needs with the privacy rights of the employee? It argues that the time has come to take on this legislative task. The pace of technological development has clearly outstripped the pace of legal developments, and it is time to catch up.

6. RONALD E. BERENBEIM, THE CONFERENCE BOARD, INC., RES. REP. No. 945, EMPLOYEE PRIVACY, at v (1990) (quoting Preston Townley, President and CEO of The Conference Board); see also OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, PUB. No. 333, THE ELECTRONIC SUPERVISOR: NEW TECHNOLOGY, NEW TENSIONS, at 22 (1987) [hereinafter THE ELECTRONIC SUPERVISOR]. ("A major decision for Congress is whether the present balance between worker rights and management requirements is reasonable, and, if not, if it can be satisfactorily accommodated through stakeholder agreement, e.g., negotiations between labor and management in government and the private sector. If the use of new technology is seen as weakening the voice of employees in such negotiations, Congress may choose to take action to ensure a reasonable balance.").

7. See Oscar H. Gandy, Jr., The Surveillance Society: Information Technology and Bureaucratic Social Control, 39 J. COMM. 61, 61 (1989). As stated in that article, "The current legal system is hopelessly inadequate to the challenge of controlling the 'technologies of control.'" Id. at 62 (citing KEVIN G. WILSON, TECHNOLOGIES OF CONTROL: THE NEW INTERACTIVE MEDIA FOR
Finally, the Article examines legislative proposals now pending before the United States Congress and presents recommendations for change.

II. ARTIFICIAL MONITORING AND SURVEILLANCE OF EMPLOYEES IN AMERICA—LEGITIMATE CONCERNS OF EMPLOYERS AND EMPLOYEES

A. An Illustrative Hypothetical

Visualize a human resources director for a major retailer contemplating a few among the multitude of personnel problems facing her employer in 1991. Everything except profits seems to be escalating. Inventory shrinkage is up markedly—the auditors say it is the employees, not shoplifters, who are the primary source of the problem. Telephone expenses are increasing at a rate not explainable by a corresponding increase in business activity. Employee medical insurance premiums are on the rise—the underwriters say a plan to decrease employee smoking might be a means to reduce premium costs. Lawsuits by injured customers are a growing concern—in one lawsuit, a customer was injured by an escalator malfunction and the employee who serviced the escalator may have been under the influence of cocaine. There has been a surge in customer complaints about slow or inadequate service.

Management, as recommended by our human resources director, then implements a comprehensive plan designed to turn the tables on these vexing problems. The plan includes a system of video surveillance of employees at work, biometric identification of employees entering and leaving the premises in order to reduce theft loss, and a telephone accounting system to reduce unauthorized personal calls. An employee "wellness" plan is implemented, including a policy prohibiting smoking both at work and away from work. Compliance is monitored by periodic pulmonary exams. A program to reduce employee drug abuse is a high priority of management and includes the testing of all new employees, and testing for cause of existing employees. In order to evaluate concerns about customer service, random monitoring of employee telephone calls is undertaken in conjunction with another system to monitor the computer keystrokes of catalog department employees.

In this era of corporate downsizing, our hypothetical human resource director ultimately loses her job as part of a reduction-in-force. She applies with a competitor of her old employer and her new employer thoroughly reviews her background, including credit history and criminal record. She is hired after successfully completing a battery of personality evaluations, pen and pencil
honesty exams, and drug tests. She is delighted to have the opportunity to travel as required by the new position but is bothered by the fact that the location and fuel consumption of all company-owned vehicles is monitored by computer. Her office includes the latest personal computing equipment but she is dismayed to learn, after having been employed for a significant time, that software installed on the personal computer network has allowed her immediate superior to review the contents of her electronic mail and fax messages, and to call up her computer screen onto his—without her knowledge of the intrusions. Her new position pays well but the corresponding demands on her personal time are greater. Her employer expects to be able to reach her at all times and provides her with a voice-activated paging system, a cellular phone in her company car, and a personal computer with a modem for home use.

The resulting increased stress level for our human resources director soon begins to cause health problems. She, as well as anyone, understands the demands that have caused her employer to implement these systems for monitoring and surveillance of its employees. Now, however, she questions whether the decrease in her motivation and productivity caused by these monitoring and surveillance techniques outweigh any potential benefits inuring to her employer.

B. Compelling Reasons for Monitoring and Surveillance of Employees

This hypothetical illustrates the plethora of legitimate, yet competing, demands that now raise a compelling question for Congress and the courts. Although it is possible that there will be illegitimate use of modern technology to carry out artificial monitoring and surveillance of employees, the compelling question at this time is, assuming legitimate employer reasons, whether our society is prepared to leave that process substantially unregulated.9

It is, of course, inevitable that some illegitimate use will occur. However, that abuse does not now appear to be occurring on a large scale. A 1987 government report considered the possibility of such abuse of computer-based monitoring of employees.10 The report specifically recognized the possibility of illegitimate uses, such as frustration of union organizing efforts, circumvention of employment discrimination laws via intensified scrutiny of protected employees, and identification of whistleblowers. That study concluded that there is no significant evidence that these abuses are occurring on a large scale or that artificial monitoring and surveillance lends itself more to illegal retaliat-

9. See generally Jeffrey Rothfeder & Michele Galen, Is Your Boss Spying on You?, BUS. WK., Jan. 15, 1990, at 74 (describing the “wide latitude for prying” given to employers by state and federal law and describing some of the many legitimate reasons employers have to engage in that prying, and labeling that scenario as “hottest employment law topic of the 1990s”); Michael A. Verespej, How Much Can You ‘Bug’ Your Employees?: It’s Becoming Increasingly Difficult to Monitor Activity On or Off the Job, INDUSTRY WK., Aug. 7, 1989, at 65 (stating that “[r]ight now the hottest of the privacy issues is electronic surveillance and monitoring”).

10. THE ELECTRONIC SUPERVISOR, supra note 6, at 102-04.
tion than other forms of technology. To the contrary, the most commonly cited employer reasons for implementing artificial monitoring and surveillance systems appear to be legitimate and are well within the acceptable scope of an ordinary employer-employee relationship.

The efforts of employers to reduce losses caused by the shocking levels of employee theft in the United States provide a persuasive example of one legitimate reason for the artificial monitoring and surveillance of employees. Studies are not in complete agreement as to the exact total amount of cash and merchandise lost each year to employee theft. Although some estimates are as high as $200 billion per year, $40 billion per year appears to be a more common estimate. In any case, the losses are enormous, and employer efforts to recoup those losses can be cost effective. In a study of the 1989 experience of a large group of major retailers, it was determined that the average value of merchandise recovered per apprehension was $1350 in the case of employee theft compared to $196 in the case of customer theft.

Theft of tangible property, however, is not the only aspect of the employee theft problem. A study by a nationwide personnel consulting firm indicates that employees of American business stole $170 billion in employer time in 1989. In addition to the efforts of employers to protect their tangible property and time, employers increasingly must take affirmative steps to protect their interests in intangible property, such as trade secrets.

11. Id.
12. See generally Elinor P. Schroeder, On Beyond Drug Testing: Employer Monitoring and the Quest for the Perfect Worker, 36 KAN. L. REV. 869, 873 (1988) (recognizing that it is "axiomatic" that employers have legitimate interests in production, discipline, and safety, which may serve as a basis for monitoring).
13. See, e.g., John W. Jones, Megatrends in Integrity Testing, SECURITY MGMT., July 1990, at 27A, 29A (reporting on a 1989 study indicating that 60% of fast-food employees and 43% of supermarket employees admit to stealing cash or property from their employers).
15. E.g., June P. Schafer et al., The Ways and Means of Screening, SECURITY MGMT., July 1990, at 20A (citing a United States Commerce Department study).
16. An Ounce of Prevention, CHAIN STORE AGE EXECUTIVE, Jan. 1991, § 2, at 4, 5 (presenting the results of an Ernst & Young annual study for the International Mass Retail Association); see also Jack Hayes, Employee Theft Is No. 1 Problem Facing Today's Busy Retailers, DISCOUNT STORE NEWS, Sept. 17, 1990, at 108 (estimating that employee theft may account for 38% to 43% of retail store inventory shrinkage and opining that this may be a low estimate); Edward M. Parker, An Inconvenient Problem, SECURITY MGMT., July 1990, at 26, 29 (reporting that the primary cause of convenience store inventory shrinkage is employee theft).
17. Arnold et al., supra note 14, at 63 (reporting a study conducted by the consulting firm Robert Half International).
18. See THE ELECTRONIC SUPERVISOR, supra note 6, at 103 n.58 (noting the necessity of monitoring the flow of information to protect employer's rights under the law of trade secrets); Christian Q. Dubia, Q & A: Christian Dubia; Attorney, McCauley & Dubia, L.A. TIMES, July 8, 1991, at D4 (reporting the rising number of unfair competition lawsuits by employers against their former employees). See generally Note, Addressing the New Hazards of the High Technology Workplace, 104 HARV. L. REV. 1898, 1899-1902 (1991) (discussing the vulnerability of corpora-
1992] ARTIFICIAL MONITORING OF EMPLOYEES 745

Although theft prevention may provide the most striking example of a legitimate reason to conduct monitoring and surveillance, there are many additional, legitimate reasons that commonly are advanced. In an era of increasing competitiveness, particularly from foreign business, the demands on employers to increase the "bottom line" renders artificial monitoring and surveillance particularly enticing.

In such an atmosphere, employers naturally seek to use technology to increase employee productivity. Monitoring and surveillance technology may increase productivity through enhanced ability to efficiently schedule personnel and equipment. Productivity increases may result from more effective evaluation of employees for periodic pay increases, promotion, termination, or transfer or by providing prompt, objective feedback to employees. Or it may result from minimizing substance abuse, both at the workplace and away from the job.

tions to computer crime). Employees are the most common culprits in computer crime cases. Id. at 1900 n.11. Congress has already enacted legislation aimed at curbing computer crime. See generally Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, 43 VAND. L. REV. 453 (1990).

19. E.g., Christopher Power et al., Value Marketing: Quality, Service and Fair Pricing Are the Keys to Selling in the 90s, BUS. WK., Nov. 11, 1991, at 132.

20. THE ELECTRONIC SUPERVISOR, supra note 6, at 91. This reason may become even more compelling in an era when many employers may perceive that the overall quality of available employees has decreased. See, e.g., Peter T. Kilborn, Unseen Sentinels in the Workplace, N.Y. TIMES, Dec. 23, 1990, § 1, at 1. Despite this perceived need to monitor for productivity reasons, studies have not clearly determined whether these monitoring systems have a positive or negative effect on productivity. See Rebecca Grant & Christopher Higgins, Monitoring Service Workers via Computer: The Effect on Employees, Productivity, and Service, NAT’L PRODUCTIVITY REV., Spring 1989, at 101, 102 (stating that “[s]ome studies suggest favorable effects on productivity while others indicate negative results”). An example of the use of artificial monitoring and surveillance to enhance productivity is the practice of sharing computer screens in a network of personal computers between the supervisor and the subordinate in order to allow training and coaching. See Fickel, supra note 1, at 50.

21. THE ELECTRONIC SUPERVISOR, supra note 6, at 91.

22. Id. Evaluations arguably can be less tainted by human bias when based on results of artificial monitoring. Kilborn, supra note 20, at 1. Also, computerized monitoring systems may be better at delivering negative information in a nonthreatening manner than a human supervisor. Grant & Higgins, supra note 20, at 101.

23. Grant & Higgins, supra note 20, at 101. Feedback may arguably be given more regularly and in closer proximity to the evaluated event when computer based systems rather than direct human observations are utilized. Id. The process of monitoring employee keystrokes and providing immediate feedback via computer is called coaching. See Marilyn Gardner, A Heroine—But Not Full Time, CHRISTIAN SCI. MONITOR, June 18, 1991, at 13.

24. See PAYTON B. SCHUR & JAMES F. BRODER, INVESTIGATION OF SUBSTANCE ABUSE IN THE WORKPLACE 11 (1990). In an “unscientific study” by the authors of approximately 6000 employees of firms that have been clients of the authors, it was determined that approximately 29% had committed company policy violations over a five-year period. Id. These violations increase workers’ compensation costs, losses due to inventory shrinkage, quality control costs, absenteeism, and litigation. Id. at 12-14. Problems of this nature led to the testing of approximately 8 million workers in 1989 and an expectation that this number will triple by 1992. Cindy Skrzyczki, Drug Testing Industry Shows Its Wares; 100 Vendors Take Part in Conference on Checking Job Applicants,
Another attractive use for monitoring and surveillance technology is to employ it as one tool to meet increasing consumer demands\textsuperscript{25} for improvements in product and service quality.\textsuperscript{26} American business is so haunted by consumer perceptions that it lags behind its foreign counterparts in this area. Again, monitoring and surveillance technology is an attractive tool to repair this perception.

Still another enticing attribute of the technology is its potential to reduce costs. These costs run the gamut from the mundane, such as the control and proper allocation of telephone expenses, to the more esoteric, such as control of employer liability under many liability theories. In addition to liability based upon the common law principle of respondeat superior,\textsuperscript{27} employers now are frequently sued by persons injured by employees based on negligent hiring, retention, and referral theories.\textsuperscript{28} First, an injured person may prevail under these theories without proof that the employee of the defendant caused injury to the plaintiff in the course and scope of that employee's employment.\textsuperscript{29} Second, these theories impose a continuing duty in the sense that they apply if the employer was negligent in either the selection process or in the ongoing employment process.\textsuperscript{30} The availability of these theories substantially increases
the impetus for employers to be meticulous in both the hiring and evaluation of employees through the use of screening and monitoring technology. In addition to potential civil liability, employers have an additional motivation to screen and monitor employees to avoid criminal responsibility. Such criminal liability may, in limited circumstances, be based on the failure of that manager to adequately supervise another employee; in the case of a corporate employer, the criminal acts of the employee may be imputed to the employer.

The possible methods of cost control offered by this technology are seemingly endless. In an era of soaring insurance premiums, consider the additional potential savings derived through monitoring worker safety. A thorough monitoring of worker safety may reduce insurance premiums, worker’s compensation claims, medical premiums, and fuel costs.

Artificial monitoring and surveillance is also a tool used to comply with many recordkeeping duties imposed by law. Many statutes place affirmative duties upon employers to collect information about employees and to maintain records of compliance with those requirements. Also, the legal obligation of an employer to protect the confidentiality of employee records, in certain


32. See F. Lee Bailey & Henry B. Rothblatt, Defending Business and White Collar Crime—Federal and State § 338 (1969) (stating that a corporation “may be criminally liable for the acts of its officers or agents done by them while exercising authorized powers”).

33. See The Electronic Supervisor, supra note 6, at 34-36 (illustrating the beneficial aspects of employee monitoring).

34. See Janet Novack, Abuse Control, Forbes, June 10, 1991, at 98. The article reports on a database developed by one major corporation that integrates the personnel, medical, and disability records of its many employees. This integrated approach to monitoring the medical experiences of its employees is designed to enable it to identify those employees who abuse medical benefits and those physicians who prescribe unnecessary tests.

35. See Rothfeder & Galen, supra note 9, at 74 (reporting that a major grocery chain places dashboard computers on its trucks to record speed, oil pressure, engine RPM, idling time, and the fact and length of stops).

36. Fair Labor Standards Act, 29 U.S.C. § 211(c) (1988) (mandating that employers keep employee records); Occupational Safety and Health Act of 1970, 29 U.S.C. § 657(c) (1988) (mandating that employers keep employee records); 1986 Immigration Reform and Control Act, 8 U.S.C. § 1324a(b) (1988) (establishing employment verification system); see, e.g., The Electronic Supervisor, supra note 6, at 103 n.55 (reporting reliance by American Express on its computerized monitoring system to ensure compliance with the Fair Credit Reporting Act); Tony Mauro & Julia Lawlor, Do Workers Have Private Lives? More Bosses Set Rules for After Hours, USA Today, May 13, 1991, at 1A (reporting on certain companies, such as transportation companies, which are required by law to test employees for drug use). See generally Kurt H. Decker, Employee Privacy Law and Practice 18-20, 455-58 (1987) (discussing these affirmative duties and providing an appendix of examples of federal statues containing record and reporting requirements that affect employee privacy).

37. See The Electronic Supervisor, supra note 6, at 94 (noting that “leakiness is a factor in determining the legality of certain information practices”).
circumstances, may be furthered by monitoring and surveillance.

C. The Nearly Irresistible Menu of Artificial Monitoring and Surveillance Options Available to Employers

There is not a precise meaning given by the law to the term "artificial monitoring and surveillance" that this Article uses to describe its subject matter. However, the menu of space-age artificial monitoring and surveillance options now available to serve the plethora of legitimate employer purposes described above is impressive in both its breadth and rate of growth. As stated in a recent news story:

To hear it from the mavens of commercial surveillance, there is no such thing as paranoia; your worst fears are probably true. If you think someone is tapping your phone calls, bugging your office or reading what's in your computer, you are probably right. The fire sprinkler in the ceiling could be a camera; the person on the phone who says she is "Judy from accounting" could be an imposter; the janitor could be a private investigator ready for a session of "dumpster diving."  

38. Grant & Higgins note:

There is no widely accepted definition of computerized performance monitoring. Terms like "worker monitoring," "electronic surveillance," "performance monitoring," and "worker surveillance" have all been used to describe various systems. According to the Office of Technology Assessment, there are three broad categories of monitoring systems: those that focus on performance, such as measuring keystrokes, use of computer time, or the content of telephone conversations; those that focus on behaviors, such as measuring use of resources, tracking of worker location via identification badges, testing predisposition to error (e.g., drug testing); and those that focus on employee characteristics, such as state of health and truthfulness.

Grant & Higgins, supra note 20, at 102. Although not limiting itself to the workplace, a recent article conveys well the breadth of the capabilities of the technology potentially falling within the scope of the term "artificial monitoring and surveillance." The author states:

These devices serve a variety of purposes, from noting the presence or absence of persons or objects to determining their identity or status, including their state of mind. Cameras now require little or no light, and microminiaturized versions can be easily hidden from sight; listening devices can hear conversations in rooms hundreds of yards away; and scientific instruments can examine bodily fluids and genetic material at the molecular level. We include here the scanners that read the Universal Products Code ("UPC") on commercial products in the supermarket as well as the infrared detectors that count the number of patrons for museum exhibits. The common quality is that these devices are more sensitive than ever before and overcome previous limits on time, space, and distance in gathering information about individuals. Associated technologies also allow for the storage, retrieval, and processing of these data gained through surveillance of the environment.

Gandy, supra note 7, at 62; see also THE ELECTRONIC SUPERVISOR, supra note 6, at 14 (stating that "all these information-gathering techniques are on a continuum with no clear boundaries").

39. Megan Rosenfeld, At Surveillance Expo, Sneak Peeks at the Sweet Spy and Buy: Helpful Hints for Those Who Snoop to Conquer, WASH. POST, Dec. 18, 1989, at F5 (reporting on some of the devices available to thwart employees trying to sell intellectual property, retaliate against a superior, or embezzle).
One result of browsing through this impressive menu is a nearly irresistible temptation to deal with the resulting legal issues by selecting one category of technology offered on the menu and addressing it in isolation. Unfortunately, this is the approach our legal system has generally taken in the past. The undesirable result has been that technology remains at least one step ahead of the law. Another disadvantage of a device-specific approach is that, as illustrated below, the categories overlap in so many respects that it becomes unduly confusing to determine what practices properly fall within the scope of the category chosen. For example, is genetic screening a medical testing technique appropriately governed by federal statutes applicable to discrimination against disabled persons, or is it properly within the scope of legislation, such as that advocated by this Article, regulating artificial monitoring and surveillance?

One common method of breaking down this complex menu into manageable categories is to distinguish between the terms “monitoring” and “surveillance.” In the workplace, the term “monitor” generally connotes observation undertaken to determine whether an employee is completing an assigned function in an appropriate manner. For example, did the sales clerk handle the transaction in an efficient and courteous manner? By contrast, other types of technology are designed primarily for surveillance purposes. The term “surveillance” generally connotes observation to determine employee behaviors and personal characteristics, such as whether an employee violated a work rule. For example, did the sales clerk pocket part of the cash proceeds of the transaction? Although distinguishing the terms may be useful for some purposes, the meaning of “artificial monitoring and surveillance” for purposes of this Article encompasses systems designed for monitoring purposes as well as systems designed for surveillance purposes. It includes but goes beyond electronic monitoring or computer-based monitoring, which is often used to refer to the electronic observation and recording of the work performed by employees on a computer keyboard.

Another frequently cited distinction in discussions of these technological developments is between work monitoring and worker monitoring. The broad definition of artificial monitoring and surveillance used in this Article includes both work monitoring (work measurement) and worker monitoring (worker testing). Work monitoring focuses on the events that actually occur in the workplace and are related to performance of services for the employer. For

---

40. For example, the federal statute regulating the use of polygraph examinations in the workplace is known as the Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009 (1988). See infra part III.A.6 (discussing the protections for employees offered by this act). This type of legislation is often referred to as “device specific legislation.”

41. See Grant & Higgins, supra note 20, at 108-09.

42. Id. at 108.

43. Id. at 109.

44. THE ELECTRONIC SUPERVISOR, supra note 6, at 13.

45. Id.

46. Id.
example, computer software used to count employee keystrokes is commonly described as work monitoring. By contrast, worker monitoring focuses on determining the individual characteristics of the employee in order to determine the employee's suitability to perform a particular function. Therefore, information gathering techniques in this worker-monitoring category include polygraph tests, drug tests, genetic tests, and brain-wave scanning.

There is obviously an overlap between work monitoring and worker monitoring in even the most basic forms. For example, a supervisor personally observing work performance and recording the results on a sheet of paper has the opportunity to both record actual output, such as the number of transactions processed, and to form opinions about characteristics of the employee likely to effect the employee's future productivity. Therefore, any comprehensive legal solution designed to deal effectively and fairly with the multitude of issues raised by artificial monitoring and surveillance in the workplace must consider forms of technology labeled as a work monitoring device or a worker monitoring device.

A distinction is also frequently made between content monitoring and transactional monitoring. Once again, aspects of both terms must be taken into account in any comprehensive solution. Monitoring may merely be undertaken to identify the specific transactions completed by an employee, but modern techniques often allow experts to use this kind of transactional information to create a personality profile or dossier concerning that individual. In other words, a sufficient quantity of transactional information may become content information.

The types of artificial monitoring and surveillance that fall within the scope of this broad definition, and that are now commonly used in the workplace, extend nearly as far as your imagination will carry you. For example, a re-

---

47. Id.
48. Id. at 14.
49. Id.
51. The Electronic Supervisor, supra note 6, at 5 (pointing out that the common practice of telephone call accounting has the potential to be used to build a "profile" of an individual employee, which could then be used to harass that employee).
52. See generally Barbara Garson, The Electronic Sweatshop ch. 8 (1988) (describing the reactions of both managers and their subordinates to various types of electronic surveillance); Shoshana Zuboff, In the Age of the Smart Machine: The Future of Work and Power 322-37 (1988) (describing the danger that various forms of modern technology will be used simply to control employees rather than to make jobs more rewarding to employees).
53. A frightening scenario of the potential of the combined use of a large number of these various techniques is presented by a hypothetical personnel policy discussed in a recent issue of the Harvard Business Review. See Gary T. Marx, The Case of the Omniscient Organization, HARV. BUS. REV., Mar./Apr. 1990, at 12. In that case the fictional employer, competing in a global market and facing the possibility of layoffs, adopts the recommendations of an employee-relations firm and implements personnel policies designed to improve productivity and quality while reducing employee turnover, health-care costs, workplace accidents, employee theft, employee drug use and leaks to competitors. Id. The policy includes multiple techniques to screen
cent news report indicates that some employers are even using special chairs to measure worker wiggling, presumably based on the premise that more wiggling means less working. Another report indicates that some employers are using subliminal messages on video display terminals to motivate workers.

It is not the purpose of this Article to advocate inclusion, at this time, of all of these techniques within the scope of the proposed legislation. Given the current status of the law, that is simply not feasible. Rather, the purpose of discussing these techniques is twofold. First, the legislation should include as many of these techniques as possible while providing flexibility to cover those we have not yet imagined. Second, review of these techniques serves to remind us that we need to consider comprehensive workplace privacy legislation encompassing all of these techniques.

When the term artificial monitoring and surveillance is used in this broad sense—any form of observation, collection of information, or analysis of data not accomplished through the sensory perception of the individual supervisor—the array of techniques in this category borders upon the overwhelming. Many of these techniques, when undertaken with the consent of the employee potential new employees and monitor existing employees. Potential and actual employees are informed of the use and the reasons behind these techniques, which even extend to employee activities away from the employer's business location. The techniques include medical and psychological testing at the entry level combined with database searching for educational, credit, automobile driving, health, military, and worker's compensation information in order to create a "predictive profile" of the potential employee; comparison of that profile to the features of the best employees; periodic pulmonary exams, urinalysis, and other medical tests to monitor long term health; subliminal messages on personal computers combined with aromatic and musical enhancement of the workplace; keystroke monitoring; video and audio surveillance; telephone call accounting and call blocking; building access systems; computerized vehicle monitoring; and the use of pagers, beepers, personal computers with modems, and fax messages to keep in contact with the employee away from the employers place of business. Id. It is tempting to think of these techniques as futuristic. However, as one of the experts who evaluated this hypothetical noted:

Dominion-Swann Industries sounds like a futuristic workplace, where life is saturated with computers that measure everything from your productivity to your heartbeat, where dreams of a perfectly ordered, clockwork world, shorn of human conflict, can come true. But DS already exists. Its technology strategy is widely adhered to. Some elements of its organizational strategy have been practiced for over 100 years. Others have been implemented and perfected throughout the 1980s.

Id. (emphasis added) (comments of Shoshana Zuboff, associate professor at the Harvard Business School and author of In the Age of the Smart Machine: The Future of Work and Power (1988)). As another of the experts evaluating that hypothetical noted, "DS's policies are discriminatory, invasive and counterproductive. And though few companies implement such an impressive package of organizational and technological measures, all of these policies exist in one form or another in American businesses—with poor results." Id. (emphasis added) (comments of Karen Nussbaum, Executive Director of 9to5, National Association of Working Women). See generally Leslie Papp, Working Under the Electronic Eye—Is It Big Brother or a Necessary Management Tool?, TORONTO STAR, July 27, 1991, at D1 (providing an analysis of recent technology and its importance to employers).

54. See Rothfeder & Galen, supra note 9, at 74.
or prospective employee, should not be within the scope of the legislative proposal analyzed by this Article. Examples include substance-abuse testing, psychological testing techniques (such as personality testing), "paper and pencil honesty examinations," polygraph examinations, and medical screenings.

56. See The Electronic Supervisor, supra note 6, at 14 (referring to the testing of "millions of private employees"). See generally Eric R. Greenberg, Workplace Testing: Who's Testing Whom?, PERSONNEL, May 1989, at 39 (reporting on a survey by the American Management Association Research Reports in December 1988 of 1005 firms demonstrating a "dramatic" increase in drug testing, i.e., 48% used drug testing in 1988 as opposed to 21% in 1986 and 37% in 1987). Most employers who test appear to test all newly hired employees and to test existing employees only for cause, but there are many variations in policies. Id.; Paul L. Blocklyn, Preemployment Testing, PERSONNEL, Feb. 1988, at 66 (reporting on a survey to which 142 human resources managers responded indicating that 18% used some form of preemployment alcohol or drug test in their business). Note that all the artificial monitoring and surveillance techniques described in this section can theoretically be used at any stage of the employment process. For example, although drug testing is more common for newly hired employees, it might also be used in the case of an application of an existing employee for a promotion.

57. See Schafer et al., supra note 15, at 23A. The financial cost to an employer of an error at the hiring stage is illustrated by the cost of replacing employees. It is estimated that it can cost from $5000 for an hourly employee to $75,000 for a managerial-level employee in lost productivity and training time when an employee leaves his employer after a few months of employment. Marlene Brown, More Than a Gut Feeling, SECURITY MGMT., Sept. 1990, at 105, 105. Similarly, other experts estimate that replacing a competent employee will cost 300 to 700 hundred times that person's hourly pay. Kate Bertrand, Hiring Tests: Sales Managers' Dream or Nightmare?, BUS. MARKETING, July 1990, at 34.

58. See Blocklyn, supra note 56, at 66 (reporting a survey to which 147 human resources managers responded, the results indicating that 20% used some form of personality or psychological testing in their business). Similarly, a 1990 survey by American Management Association Research Reports using a much larger sample reported that 20.6% of employers use psychological or behavioral testing. Justin Martin, Workplace Testing: Why Can't We Get It Right?, ACROSS THE BOARD, Dec. 1990, at 33, 35.

59. There has been an upsurge in the use of "paper and pencil honesty tests," or "integrity tests." The reasons for this increase include increasing liability concerns of former employers in conveying information to new employers and the passage of the Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001-2009 (1988), and similar state legislation. See Robert Moore & Robert M. Stewart, Evaluating Employee Integrity: Moral and Methodological Problems, 2 EMP. RESPS. & RTS. J. 203, 204 (1989); see also, e.g., Martin, supra note 58, at 66 (1990 survey by American Management Association Research Reports drawing from a sample of 1021 companies in eight industries showed that 16.4% use pencil and paper honesty testing). However, some testing experts express serious concern about the predictive capability of these tests. Id. at 213-14. See generally Robin Inwald, Those "Little White Lies" of Honesty Test Vendors, PERSONNEL, June 1990, at 52, 52 (arguing that properly designed written tests are one of the best sources of data upon which to base hiring decisions but also pointing out their limitations, the potential for unfairness, and the excessive claims as to their reliability being made by vendors). By contrast, other experts argue that they are highly reliable and that the upsurge in use has occurred because they are a nondiscriminatory and reliable device that may be used by employers as an effective response to increasing losses due to employee dishonesty. Arnold et al., supra note 14, at 63-64; Bertrand, supra note 57, at 34.

60. See The Electronic Supervisor, supra note 6, at 14 (reporting 2 million exams annually by 1990); Blocklyn, supra note 56, at 66 (reporting a 1988 survey to which 147 human resources managers responded, indicating that 11% used some form of lie detector, psychological stress evaluator, or honesty test for employment applicants in their businesses). But see Martin, supra
ARTIFICIAL MONITORING OF EMPLOYEES 753

ing,61 screening of employees for high cholesterol levels,62 genetic screening63 and mapping,64 brain wave testing,65 credit reports (including "investigative

note 58, at 35 (reporting a 1990 survey by American Management Association Research Reports indicating that only 3.7% of employers now engage in polygraph testing). The use of the polygraph is expected to decline dramatically following the passage of the Employee Polygraph Protection Act of 1988. See Greenberg, supra note 56, at 41.

61. See Frank Swoboda, Ripe for Discrimination: Medical Risks, WASH. POST, Apr. 8, 1990, at H3. A substantial number of employers use medical screening. Some reports estimate that as many as nearly one-half of all employers use medical screening. Id. It is, however, relatively rare for employers to test for HIV antibodies. E.g., Greenberg, supra note 56, at 43 (reporting a survey of 1005 firms by the American Management Association Research Reports in December 1988, which found that testing for the presence of HIV antibodies, commonly called AIDS testing, is relatively rare, with only 7.5% of the respondents indicating that they utilize such tests).


63. These tests are designed to identify specific genetic traits that render the individual tested particularly susceptible to certain diseases, such as cancer. In other words, they do not test whether an individual has a disease or has chosen to engage in behavior likely to cause them to contract a disease but instead test whether that person's particular genetic makeup renders it likely that they will be stricken. See Ellen Pierce, The Regulation of Genetic Testing in the Workplace—A Legislative Proposal, 46 OHIO ST. L.J. 771 (1985) (proposing a specific federal statute to regulate this practice); see also THE ELECTRONIC SUPERVISOR, supra note 6, at 14 (reporting that this type of screening was only being used in a "few workplaces" in 1990); Hoerr, supra note 28, at 61 (reporting the potential of these tests to indicate a prospective employee's genetic predisposition to certain diseases but concluding "that as far as anyone knows, no companies now use the tests to deny employment"); Genetic Check for Jobs, NEWSWEEK, Oct. 13, 1991, at 16 (reporting a range of $200 to $1000 for tests and that few employees are using them, but pointing out that rising health-care costs could change that pattern). Legislation is pending in Congress that would regulate this area in a limited manner. See H.R. 2045, 102d Cong., 1st Sess. (1991). This proposal, introduced by Rep. John Conyers, is known as the Human Genome Privacy Act. It has been referred to the House Government of Operations Committee. 137 CONG. REC. H2534 (daily ed. Apr. 24, 1991). The proposal is similar to the Privacy Act of 1974, 5 U.S.C. § 552(a) (1988), in the sense that it would apply only to genetic information maintained by the federal government and would protect the privacy rights of individuals with respect to genetic information in the hands of the federal government.

64. The “human genetic landscape” is known as our genome. Robert A. Weinberg, The Dark Side of the Genome, TECH. REV., Apr. 1991, at 44, 45. Scientists have undertaken the process of mapping this landscape and identifying variations known as polymorphisms. Scientists then look for associations between these polymorphic markers and specific traits of individuals. Id. at 45. For example, researchers have already identified the polymorphic marker leading to Huntington's disease. Id. What dangers does this create in the workplace? See generally Tom Fennell, Nearing the Final Frontier: Science Can Re-Engineer the Embryo, MACLEAN'S, July 15, 1991, at 37 (raising the possibility that discrimination based on genetics could occur in the workplace); Daniel F. Jennings, Is Genetic Testing Legitimate Screening or Discrimination, AM. PAPERMAKER, Sept. 1991, at 56; Jennifer Landes, Sides Drawn Up on Genetic Testing, NAT'L UNDERWRITER, Dec. 10, 1990 (Life & Health/Fin. Services ed.), at 2 (discussing the potential for discrimination on prohibited bases due to genetic testing). Experts predict that this decade will bring the ability to predict by routine tests the predisposition of individuals to certain diseases (e.g., cancer, Alzheimers, diabetes) and the likelihood that individuals will develop certain traits (e.g., intelligence, moodiness). Weinberg, supra, at 45.

This sort of information has enormous potential economic value to employers who are worried about the skyrocketing costs of employee health insurance plans, the susceptibility of individual employees to dangers such as chemicals in the workplace, and maintaining the most qualified workforce possible. Experts, however, do not agree on the likely accuracy of these genetic screen-
testing for specific job-related skills, pulmonary capacity testing devices. E.g., Employers Shouldn't Use Gene Tests: AMA Report, NAT'L UNDERWRITER PROP. & CASUALTY, Oct. 14, 1991 (Risk & Benefits Mgmt. ed.), at 49 (reporting on an American Medical Association report advising employers not to use genetic tests as a condition for employment); Rochelle Green, Discrimination by DNA: Possible Consequences of Genetic Testing, HEALTH, Jan. 1990, at 86 (reporting the opinion of a geneticist that genetic information is an unreliable predictor of risk). Therefore, the possibility exists that workers will be excluded from employment, treated less favorably on the job, or terminated due to their genetic predisposition, which may or may not be an accurate predictor of future performance. Apparently, this dire scenario has not yet materialized. A recent study by the United States government shows little current use of genetic testing in the workplace and little change in use since 1982. OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, PUB. NO. 455, GENETIC MONITORING AND SCREENING IN THE WORKPLACE 22-23 (1990); see also David Brown, Individual 'Genetic Privacy' Seen as Threatened; Officials Say Explosion of Scientific Knowledge Could Lead to Misuse of Information, WASH. POST, Oct. 20, 1991, at A6 (discussing Office of Technology Assessment Report); Thiel, supra note 62, at 44 (reporting that there is little evidence to date that employers are abusing this technology); Few Employers Use Genetic Screening or Monitoring, Despite Improved Tests, GENETIC TECH. NEWS, Feb. 1991, at 3. However, some employers are now using genetic testing. E.g., Richard Saltus, Bias Issue Looms over Insurers; Creating Another Underclass, BOSTON GLOBE, Nov. 12, 1990, at 33 (reporting on an employee excluded from his employer's health insurance plan because of a mutant gene carried by both the employee and his son). Further, it is likely that a surge in use by employers will take place as the tests become more affordable. See Mary Sit, Will Genetic Mapping Threaten Workers' Privacy?, BOSTON GLOBE, Aug. 21, 1990, at 23 (reporting that genetic tests for inherited illness now cost $2000 to $3000 per test, but the cost per test will soon be lowered to about $100 for certain tests).


65. See THE ELECTRONIC SUPERVISOR, supra note 6, at 14 (although in the research stage at the time of that report, predicting that mapping could be used to predict illness or to determine an employee's concentration ability).

66. See Mauro & Lawlor, supra note 36, at 1A (reporting that the limitations in federal law on the use of polygraphs in employment decisions has increased reliance on the use of credit checks). See generally Jeffrey Rothfeder, Is Nothing Private? Computers Hold Lots of Data on You and There Are Few Limits on Its Use, BUS. Wk., Sept. 4, 1989, at 74 (discussing the lack of effective limits on the use of credit reports).
to monitor smoking habits, monitoring of employee weight, criminal record checks, and reports concerning an employee's history of prior worker's compensation claims. These techniques are beyond the scope of this legislation because it simply is not practical to envision such comprehensive workplace privacy legislation in the immediate future. However, it is possible to envision such legislation being enacted in the long term, and sight should not be lost of the fact that all of these techniques are elements of a single workplace privacy problem.

These numerous exclusions do not, however, leave an insignificant number of common practices to be regulated by the proposed law. Telephone monitoring is perhaps the most obvious inclusion. It includes both call accounting and service observation. Telephone call accounting involves monitoring of the time, duration, destination, and cost of telephone calls for many purposes, including limiting personal phone use by employees. Such monitoring has been made possible on a large scale by the proliferation of new communication technology such as digital private branch exchanges, known as PBXs. Telephone monitoring is perhaps the most obvious inclusion. It includes both call accounting and service observation. Telephone call accounting involves monitoring of the time, duration, destination, and cost of telephone calls for many purposes, including limiting personal phone use by employees. Such monitoring has been made possible on a large scale by the proliferation of new communication technology such as digital private branch exchanges, known as PBXs.72 Telephone monitoring is perhaps the most obvious inclusion. It includes both call accounting and service observation. Telephone call accounting involves monitoring of the time, duration, destination, and cost of telephone calls for many purposes, including limiting personal phone use by employees. Such monitoring has been made possible on a large scale by the proliferation of new communication technology such as digital private branch exchanges, known as PBXs.72
phone service observation, by contrast, refers to actually listening in on the telephone calls of employees and recording these calls.

Computer-based monitoring, such as counting of the number of keystrokes by an employee, is also widely used and appropriately within the ambit of the proposed legislation. The development of software to "integrate" a series of individual personal computers into one "network" and then to allow the monitoring of the activities of the individuals working on those computers has made this feasible on a large scale. Some of the available software allows managers to "share screens" with their subordinates, in some cases without the subordinates' knowledge.

In addition to telephone and computer based monitoring, a wide variety of additional techniques allow the employer to track employee activity, often without the employee's knowledge that the surveillance is taking place or that records are being maintained. Computerized systems are often designed to replace manually processed time cards and to allow supervisors to monitor employee activity, including time spent on breaks. For example, these systems

recording, which accounts for the telephone that was the source of the call, the access code used to make the call, the telephone to which the call was made, and the duration of the call).

74. See Merrill Goozner, Phone Monitoring—A Fairness, Privacy Call, CHI. TRIB., Aug. 27, 1990, § 3, at 1 (reporting on the common practice of supervisors secretly listening in on the phone calls of subordinates); Robert P. Hey, ACLU Says Laws Needed to Ensure US Workers Privacy On and Off Job, CHRISTIAN SCI. MONITOR, Dec. 28, 1990, (United States), at 4 (reporting on the common practice of listening in on workers' calls in the telephone and travel industries without telling the worker).

75. See Sharon Danaan, 9to5, WORKING WOMEN'S EDUCATION FUND, INC., STORIES OF MISTRUST AND MANIPULATION: THE ELECTRONIC MONITORING OF THE AMERICAN WORKFORCE 1-2 (1990) (reporting on various types of computer-based monitoring such as nurses who carry small computers to enter procedure codes with their efficiency level analyzed based on time spent per patient). See generally THE ELECTRONIC SUPERVISOR, supra note 6, at 27-58 (discussing in detail the kind of work typically subjected to this monitoring and the extent to which this is now being undertaken in the American workplace).

76. Often known as local area networks or LANs.

77. Tara Sexton & Bob Enyart, LAN Remotes vs. the Rights of Privacy; Remote Data Base Servers, PC Wk., Mar. 27, 1989, at 56. An advertisement for this type of software in a computer magazine recently touted this product as follows:

"Close-Up LAN brings you a level of control never before possible. It connects PCs on your network giving you the versatility to instantly share screens and keyboards.... You decide to look in on Sue's computer screen. . . . Sue won't even know you are there! . . . All from the comfort of your chair."

Marx, supra note 53, at 30 (comments of Karen Nussbaum, Executive Director of 9to5, National Association of Working Women, quoting an advertisement in the March 13, 1989, issue of PC Week); see also THE ELECTRONIC SUPERVISOR, supra note 6, at 5 (noting that network systems provide a broad capacity to monitor work performed at computer terminals); Gene Bylinksy, How Companies Spy on Employees, FORTUNE, Nov. 4, 1991, at 131 (discussing "Peek," which permits supervisor access to employee screens with employee approval, and "Spy," which can allow that access without employee approval).

78. Fickel, supra note 1, at 50 (describing the "notification option" software now commercially available).

79. See Peter Krahe, Computers Put New Punch in Time Clocks, PERSONNEL J., Feb. 1989, at 46 (reporting that these systems allow the supervisor to simply ask the system "Who's there?" at
may be programmed to prevent employees from logging in earlier than the time at which they are scheduled to begin work.\textsuperscript{80}

Similar monitoring devices on employer-owned vehicles permit employers to determine length and location of stops, fuel consumption, and similar information.\textsuperscript{81} Even more sophisticated techniques are becoming available, such as computerized access control systems for building security\textsuperscript{82} and biometric identification systems.\textsuperscript{83} All these techniques are appropriately within the scope of the proposed legislation. Other techniques appropriately covered include taking still photographs of employees, video surveillance,\textsuperscript{84} reviewing files maintained by employees in personal computers at work, intercepting electronic mail or fax messages sent to or received by employees,\textsuperscript{85} and hidden any time in order to determine all employees clocked in and all those absent).

80. Id. at 49.

81. See Rothfeder & Galen, supra note 9, at 74 (reporting the use of dashboard computers on trucks). A recent article indicates that some employers are also using satellite technology to track company owned vehicles. Marx & Sherizen, supra note 26, at 62.

82. See Dave Jensen, Inside Job: Employers Boost Worker Surveillance with High-Tech Tools, BUS. J. MILWAUKEE, Nov. 5, 1990, § 2, at 9. These systems not only allow the employer to control access but also to keep records of employee movements on the premises. A system of this type with two cameras, a monitor, and a time-lapse recorder capable of 960 hours of tape can cost as little as $3200. Id.

83. The unique biological characteristics or behavioral characteristics of any individual allow scientists to identify that individual by reference to those characteristics. These identifying characteristics include retinal blood vessels, hand geometry, fingerprints, and vocal intonation. Although these biometric identification systems have been technologically feasible for many years, they are now used more widely in the workplace because the price is dropping. See, e.g., Jon W. Toigo, Biometrics Creep into Business, COMPUTERWORLD, June 11, 1990, at 75 (discussing how biometric systems are gaining popularity in the workplace); ASA ClocKeeper Software To Be Integrated with Software House Security Management Systems, Bus. Wire, Sept. 18, 1990, available in LEXIS, Nexis Library, BWIRE File (reporting on integrated software now available to control access and monitor timekeeping and employee activities).

84. See Jensen, supra note 82, at 9 (reporting on the various methods of conducting this surveillance, including a camera disguised as a sprinkler head or a heating duct). At times, the employer accomplishes the surveillance in a two-step process. The first step is a hidden camera to detect theft; the second step is a visible camera to deter theft. Id. In a recent study, this practice was reported to be more common among the United States firms responding to a survey than among the Canadian and European respondents. However, videotaping away from the workplace was reported to be less common than videotaping at the workplace. BERENBEIM, supra note 6, at 9.

85. It is estimated that as many as 10 million Americans now use electronic mail on the job. Jim Simon, Computer Privacy at Issue in Suit, SEATTLE TIMES, Sept. 17, 1990, at D1. Some of those workers are now bringing lawsuits challenging the right of their employers to look into their electronic mail files. See id. (Washington state employee sued his employer alleging it looked into his private computer files wrongfully in connection with an investigation of improper use of state computers); Michael Stroud, Rise of Electronic Mail Raises Sticky Privacy Issues, INVESTOR'S DAILY, June 22, 1990, at 13 (California lawsuit against a major computer maker). Similar issues to those being raised in these lawsuits challenging the right of employers to inspect electronic mail are likely to arise in connection with employer inspection of voice mail and faxes. Alice LaPlante, Is Big Brother Watching?, INFOWORLD, Oct. 22, 1990, at 58. It is not clear whether privately maintained electronic mail systems are covered by the protection of the Electronic Communications Privacy Act of 1986 or whether the employee has a reasonable expectation of privacy in
microphones. Excluded from the legislative proposal would be the relatively common practice of conducting physical searches of employees, employee desks, and lockers and containers in the possession of employees. Searches would not, however, be excluded if conducted by artificial means without employee consent. Such an example is the use of a remote camera or sensing device to observe an employee. Finally, the potential exists that all this information about employees from various sources may be placed into integrated databases and used to analyze the employee. If this information is originally collected in a manner subject to the proposed legislation, its later storage and analysis should be covered as well.

A comprehensive legal solution is sorely needed to address the use of these many techniques in the workplace. The solution should not be limited to the impact of these techniques upon employees alone. Rather, the solution should consider the impact of artificial monitoring and surveillance activities on non-employees who may be adversely effected by the monitoring. For example, these techniques may affect applicants for employment or customers.

The legal approach to artificial monitoring and surveillance in the workplace must also address techniques designed to promote certain types of employee behavior. For example, subliminal messages may appear on personal computer screens to encourage particular employee activity, music may be broadcast throughout the workplace to induce a particular mood, or aromas designed to create particular employee reactions may be released into the workplace atmosphere. As these examples of subliminal suggestion illustrate, electronic mail files at the office under common law privacy concepts. See generally The Electronic Supervisor, supra note 6, at 11 (reporting that all the employers interviewed believed that they had the right to search employee diskettes for personal or unauthorized company information); Evelyn Richards, Privacy at the Office: Is There a Right To Snoop?; Lawsuit May Set Limits on Firms' 'Eavesdropping,' WASH. POST, Sept. 9, 1990, at H1 (discussing the many legal uncertainties concerning the balance of employer and employee rights in this area).

86. See Marx & Sherizen, supra note 26, at 62 (reporting the hidden use of microphones in the bathrooms of a large manufacturing company to detect drug sales).

87. See Berenbeim, supra note 6, at 9. This report indicates that the United States firms responding to a survey were more likely than their Canadian and European counterparts to search lockers, desks, or offices or to examine briefcases or handbags when employees enter or leave the building. Physical searches of employee lockers, desks, or offices was the only practice used by a majority of the respondents in the United States, Canadian, and European samples. Id.

88. See Novack, supra note 34, at 98 (reporting the use of integrated databases concerning employee medical experiences).

89. E.g., Bob Dart, 79% of U.S. Workers Say Bosses Asked Them Nosy Questions, ATLANTA CONST., Jan. 10, 1990, at A1 (reporting a survey entitled Whose Business Is It Anyway commissioned by the National Consumers League in which 79% of the respondents indicated that they had been asked personal questions they considered off-limits during the job interview).

90. E.g., Marx, supra note 53, at 14 (reporting the availability of a computer program known as "Subliminal Suggestions and Self-Hypnosis" that enables managers to send messages to workers, such as "work rapidly but carefully," without the employees' knowledge); Gary T. Marx, Do Scents Make Sense as a Way To Make Us Work Harder?, NEWSDAY, July 6, 1990, at 67, 67 (reporting the availability of aromatic equipment to pump scents through air conditioning and heating ducts to promote workplace productivity).
monitoring and surveillance is often undertaken for the most laudable of purposes, say stress reduction. Any good intention does not, in and of itself, argue for lack of regulation. The employer’s intent may be at odds with that of the employee yet nevertheless imposed without the employee’s knowledge.

In designing an appropriate legal solution, it is critical to recognize that these forms of monitoring and surveillance do not occur only at the employer’s place of business. As technology lessens the necessity for many types of work to be carried out at the employer’s place of business, the monitoring might occur through the use of a beeper or by a computerized monitoring system controlled by an access code. This is, in many ways, a logical extension of the practice of adopting company policies limiting certain dating, political campaigning, and other employee activity away from the workplace. The legal solution must, therefore, recognize that the workplace is no longer limited to a specific physical structure, such as a factory. It potentially includes the employee’s car, home, and places of recreation.

The potential reach of the above-discussed artificial monitoring and surveillance techniques presents a strong argument for comprehensive workplace privacy legislation. However, it is likely impractical to expect the enactment of such legislation in the near future. Accordingly, a legislative solution to the problem at this time should address artificial monitoring and surveillance in the broad sense but should also provide appropriate exceptions for technology now subject to significant regulation by specific statutes, such as polygraph exams and credit reports. In addition, further exceptions must be provided for technologies that, like genetic testing, Congress needs more time to fully evaluate. This should be accomplished with the knowledge that it is a stop-gap measure and that the appropriate long-term solution is comprehensive worker-autonomy legislation. The most dramatic support for comprehensive worker-autonomy legislation, however, is the growing presence of this technology in the workplace.

D. Swelling Ranks of Employees Subject to Artificial Monitoring and Surveillance

A 1987 report by Congress’ Office of Technology Assessment estimated that, at the time of the report, approximately four to six million office workers in the United States were being evaluated based on computer generated statistics. Although workers performing repetitive tasks were reported to be the

91. E.g., Marx, supra note 53, at 14 (describing the possibility of monitoring an employee who uses a home computer, or using an electronic transmitter to keep track of an employee’s location).
92. E.g., Hey, supra note 74, at 4 (reporting the capability of monitoring workers off the job by computers, video cameras, access codes, pagers, beepers, and substance tests).
93. E.g., Berenbeim, supra note 6, at 10 (reporting that the survey found restrictions on intimate employee behavior to be rare but reporting the existence of some company policies in the United States prohibiting dating of other employees or employees of competitors or banning marriage to those persons).
94. The Electronic Supervisor, supra note 6, at 5.
primary subjects of computer-based monitoring, it is likely that workers at all levels will soon be monitored in this manner and on a large scale. The Office of Technology Assessment estimate encompassed only computerized monitoring. It is likely that many millions were at that time already being artificially monitored through telephone call accounting systems. In addition, there were certainly a substantial additional number of employees then being monitored by other forms of high technology monitoring, such as video surveillance.

Another estimate of the number of Americans being monitored artificially in the workplace was prepared by 9to5, Working Women Education Fund, in a 1990 report. At the time, the organization estimated that ten million workers in America were being evaluated by computer-based work monitoring. Some experts say that the number has likely doubled since the time of that study.

Another survey was conducted in 1989 by the Massachusetts Coalition on New Office Technology. That was a survey of 686 office workers employed by forty-nine different employers in the Boston area. The survey reported that 85% were subjected to computer monitoring, 81% had supervisors who listened in on telephone conversations with customers, and 45% had supervisors with the capability of monitoring conversations among co-workers through microphones on their headsets. Only 47% of those subject to these activities learned of the existence of the monitoring from their employer. The others learned from co-workers, unions, or other sources or in the course of disciplinary action by their employer.

Another indication of the widespread nature of these practices is contained in the Conference Board Report, which is based on a survey conducted by the Conference Board, Inc., a not-for-profit business information service. The

95. Id. ("[I]t is likely that computer-based monitoring will affect a large number of workers at all organizational levels."); Grant & Higgins, supra note 20, at 101 (reporting that monitoring by computers has expanded to persons including stockbrokers, pharmacists, and nurses); Marx, supra note 53, at 30 (according to Karen Nussbaum, Executive Director of 9to5, National Association of Working Women, "higher professions" are now being monitored artificially); Marlene Piurro, Employee Performance Monitoring . . . or Meddling?, MGMT. REV., May 1989, at 31, 33 (describing the manner in which management, by using software to maintain their personal schedules, make themselves susceptible to the same sort of monitoring as other workers).

96. According to Rep. Don Edwards of California, in 1987 approximately 14,000 employers listened in on telephone conversations of approximately 1.5 million employees, and most of those employees were not aware that they were being monitored. See Rothfeder & Galen, supra note 9, at 75.

97. See DANAAN, supra note 75.

98. Id. at 1. A recent article quoting the executive director of that organization states that 10 million workers are now evaluated by computer-based systems while 26 million United States workers have their work tracked electronically. Markoff, supra note 50, at 7.


100. Simson Garfinkel, Employees' Attitudes About Monitoring, PRIVACY J., June 1989, at 5 (summarizing the results of that survey).

101. Id.

102. Id.

103. See BERENBEIM, supra note 6.
survey consisted of 393 United States, Canadian, and European firms. Despite the fact that a high percentage of the respondents to that survey found the use of employee searches to be ineffective or counterproductive, the survey concluded that the techniques are fairly widespread, particularly in the United States.  

Further evidence of the widespread nature of these techniques in the American workplace is provided by another 1990 report, *The Equifax Report on Consumers in the Information Age.*  

Although *The Equifax Report* addresses only a few of the techniques discussed above, its findings concerning American attitudes towards workplace intrusion into the private lives of employees are relevant to the inquiry of this Article. The findings indicate a relatively widespread assumption that such activity occurs and that there is a relatively high acceptance of that activity under certain limited conditions. Specifically, despite this acceleration in the use of artificial monitoring and surveillance in the workplace, the findings of the report indicate that the American public is cognizant of the legitimate informational needs of employers and willing to accept certain forms of intrusion if basic fairness is assured. As stated in an analysis of the survey results by noted privacy expert Prof. Alan F. Westin, “Though concerned about threats to their privacy and distrustful of institutions in general, the Equifax survey demonstrates that the public accepts the disclosure of personal information when consumers feel that the basic principles of fair information practices outlined earlier in this essay are observed.” The survey yielded the following results.

1. Eighty percent of the members of the public and 74% of the human resources executives surveyed think that it is appropriate for an employer to check whether an applicant for employment has a criminal record.

2. Fifty-five percent of the members of the public and 38% of human resources executives surveyed think that it is appropriate for an employer to ask that an applicant take a written honesty test.

3. Forty-six percent of the surveyed members of the public, in contrast to 23% of the human resources executives, think that it is appropriate for an employer to ask that an applicant take an AIDS test.

4. Twelve percent of the members of the public and 6% of human resources executives surveyed think that it is appropriate for an employer to check into the applicant’s lifestyles or political associations. In practice, the actual rate of inquiry during the application process into these off-the-job mat-

---

104. *Id.* at 9.

105. EQUIFAX, INC., *THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE* (1990) [hereinafter *THE EQUIFAX REPORT*]. This report was based on a survey commissioned by Equifax and undertaken by Louis Harris & Associates and Dr. Alan F. Westin, professor of public law and government, Columbia University.

106. *Id.* at XXIII.

107. *Id.* at 31.

108. *Id.*

109. *Id.*

110. *Id.*
ters appears to be relatively low. The human resources executives surveyed reported as follows: 33% inquire about hobbies, 17% about marital status, 4% about smoking off the job, and 1% or less about unmarried applicants' living arrangements with persons of the opposite sex who are not family members, and about applicants' child bearing plans, elderly parents, and religious preferences. Even more rarely do human resource executives report that it would be appropriate to deny employment or to fire someone for unusual off-the-job activities. For example, only 6% of those executives think it would be appropriate to fire or deny employment to someone for such activity as working in a bar, and only 7% of human resources executives think it would be appropriate to require an employee to quit smoking.

(5) Eighty-three percent of the members of the public surveyed felt that an employer should be able to require a drug test in the application process for a job like that individual's own job. Eighty percent of the human resources executives surveyed felt this would be justified for management employees, and 82% of those executives felt this would be justified for nonmanagement employees. However, only 66% of the public felt that a random drug testing program for all employees would be justified. Fifty-three percent of human resources executives felt such a program would be justified for management employees and for nonmanagement employees.

(6) Both 58% of the members of the public and 78% of human resources executives surveyed agreed with the proposition that companies should be able to listen in on phone operators to see if they are courteous and efficient.

(7) Sixteen percent of the members of the public surveyed felt that they have been asked for information by their employer about which the employer had no right to inquire, and 7% felt that personal information about them had been used by an employer.

Despite the existence of the studies discussed above, it is obviously difficult if not impossible to state the actual number of employees in America who are subjected to artificial monitoring and surveillance in the workplace, as that term is used in this Article. It seems certain, however, that the number is very large and that it constitutes a significant portion of the workforce.

Furthermore, it appears that these estimates represent a relatively recent surge in this type of activity. Although the reasons for this trend are numer-
ous, the primary cause is evident. The surge can be attributed mainly to the change of the United States economy from a production-oriented economy to a service-oriented economy, combined with the automation of the workplace for these new service workers. The workplace is simply easier to monitor now.

Another factor contributing to this trend toward increased monitoring is the lack of legal limitations upon employers in this area. Although labor unions may bargain for such limitations as part of the collective bargaining process,\textsuperscript{119} the number of unionized workers in the United States is small\textsuperscript{120} and decreasing. Furthermore, increased sales efforts of manufacturers of the hardware and software necessary to accomplish artificial monitoring and surveillance of employees has likely played a significant role in increased use of those techniques.\textsuperscript{121}

Despite this trend toward the increased use of artificial monitoring techniques, there are signs that some employers are concluding that the negative effects of artificial monitoring outweigh its benefits and are consequently reducing its use.\textsuperscript{122} Rather than a magic solution to problems such as those

\begin{itemize}
  \item\textsuperscript{119} For example, the union representing the workers at a major United States corporation recently negotiated a collective bargaining agreement on behalf of those workers, which provided them with significant protection from the adverse effects of artificial monitoring. This agreement included a requirement that supervisors notify employees who are to be monitored for purposes of job assessment and a provision allowing employees the choice of remote monitoring or direct monitoring by a supervisor. See Kilborn, \textit{supra} note 20. Due to the significant decrease in the unionized segment of the United States workforce in recent years, this type of protection is not available to a large percentage of the workforce. See infra note 120 and accompanying text (stating that the number of unionized workers is decreasing).

  \item\textsuperscript{120} Approximately 12\% of United States workers are unionized. Gene Koretz, \textit{Why Unions Thrive Abroad—But Wither in the U.S.}, \textit{Bus. Wk.}, Sept. 10, 1990, at 26, 26; see also \textit{The Electronic Supervisor}, \textit{supra} note 6, at 5-7, 9 (OTA estimating that 20\% of the United States workforce was unionized in 1987). Fewer office workers, who are now among the most likely to be monitored artificially, are unionized. \textit{Id.} at 9. The unionized portion of the United States workforce in 1990 was one-third of that in the mid-1950s and dropping at a rate far more rapid than the rest of the world. See Koretz, \textit{supra}, at 26; \textit{The Electronic Supervisor}, \textit{supra} note 6, at 98 (reporting a decline in unionized portion of nonagricultural labor force in the United States from 35.5\% in 1945 to below 19\% in 1987, with an expected additional decline over the next 15 years).

  \item\textsuperscript{121} \textit{See The Electronic Supervisor}, \textit{supra} note 6, at 98-99 (referring to the tendencies of some vendors to "puff").

  \item\textsuperscript{122} See, e.g., Aaron Bernstein, \textit{How To Motivate Workers: Don't Watch 'Em}, \textit{Bus. Wk.}, Apr. 29, 1991, at 56, 56 (reporting that the "search for quality is abridging this trend" toward electronic eavesdropping); Kilborn, \textit{supra} note 20, at 1 (reporting that a federal government agency has recently changed its eavesdropping practices in response to employee complaints); see also Bernard Wray, \textit{Electronic Monitoring in the Workplace}, \textit{N.Y. L.J.}, Aug. 28, 1990 at 2 (reporting that the Secretary-Treasurer of the Committee on Labor Relations of the New York County Lawyers Association claimed that "[t]here simply is no credible evidence or factual or statistical proof that electronic monitoring and surveillance have achieved any positive results for employers").
\end{itemize}
faced by our hypothetical human resources director described in the Introduction, some employers are finding that artificial monitoring and surveillance is burdened with its own set of problems, and they are deciding to scale back.\footnote{123} Reasons for scaling back include worker resistance, resulting in unionization efforts or loss of key employees to other employers; decreased quality of product resulting from lower employee morale; and simple increased management sensitivity to employee concerns. Additionally, artificial monitoring and surveillance simply may not deliver the promised results. Some employers have experienced increased employee turnover rates,\footnote{124} increased employee absenteeism, increased employee health problems, decreased productivity,\footnote{125} decreased product quality, and poor customer service.\footnote{126}

For example, the Conference Board Report\footnote{127} brings into serious question the effectiveness of the use of these artificial monitoring and surveillance techniques. The report stated that "[m]ore than two-thirds of the respondents said that searches and electronic surveillance of employee conduct were ineffective or counterproductive."\footnote{128} The reasons cited by those respondents for that conclusion were "the harmful impact on employee morale," litigation exposure, and inconsistency with the philosophy of the business.\footnote{129} This apparent aversion to these techniques is stronger, however, for the Canadian and European firms surveyed than for the United States firms.\footnote{130}

Employers should also consider that the use of artificial monitoring and surveillance without adequate advance planning may create significant liability exposure.\footnote{131} Although there are not to this date a large number of reported

\footnotesize{123. A recent article cites a number of examples of major United States businesses that recently have found electronic monitoring to be counterproductive and therefore have eliminated the practice. See Piturro, supra note 95, at 32; see also Marx & Sherizen, supra note 26, at 64 (pointing out the possibility that the adversarial relationship created by artificial monitoring and surveillance of employees may cause it to become counterproductive); Wray, supra note 122, at 2 (citing the types of "bad results" from electronic monitoring observed by a labor lawyer in his practice).

124. See Kilborn, supra note 20 (discussing the connection between high employee turnover rates and increased surveillance).

125. Employees may, in fact, fight the system by doing less work because the monitoring system is in place. \textit{Id}.

126. See, e.g., Rebecca A. Grant et al., \textit{Computerized Performance Monitors: Are They Costing You Customers?}, \textit{Sloan Mgmt. Rev.}, Spring 1988, at 39 (concluding that computerized monitoring may cause workers to place a higher value on production than on customer service and teamwork, and that this may well decrease significantly the quality of customer service delivered); Peter A. Susser, \textit{Modern Office Technology and Employee Relations}, \textit{Employment Rel. Today}, Spring 1988, at 9, 10-11 (arguing that new technology may lead to poor customer service).

127. See Berenbeim, supra note 6, at 9.

128. \textit{Id}.

129. \textit{Id}.

130. \textit{Id}. The survey found that 85\% of the Canadian and European firms responded that these techniques were ineffective or counterproductive. A substantial percentage of the United States respondents had the same view, but 23\% of United States firms said searches could be somewhat or highly effective. \textit{Id}.

131. See Hoerr, supra note 28, at 61 (providing examples of "huge jury awards" in recent}
appellate court decisions upholding violation-of-privacy awards for employees, there has been a dramatic increase in the number of workplace privacy suits filed and in the size of favorable verdicts for successful plaintiffs.\textsuperscript{132}

Despite these potentially negative consequences, and the possibility that the most easily monitored jobs may well be automated out of existence, the factors promoting the use of systems for workplace monitoring and surveillance make it likely that, absent restrictive legislation, there will be a continued increase in use of artificial monitoring and surveillance in the workplace.\textsuperscript{133} The relatively low purchase cost of artificial monitoring and surveillance systems may well be the largest factor.\textsuperscript{134} Furthermore, the maintenance of these systems is not labor intensive. In addition to the cost factor, the role of organized labor as a limiting factor will decrease as labor unionization rates continue to drop.\textsuperscript{135} Those rates are particularly low in the areas where monitoring is most likely to be used, such as office work. Finally, increasing market competitiveness correspondingly increases the incentive to use artificial monitoring and surveillance.

Given the simple fact that many "[c]ompanies find it difficult not to monitor

privacy cases arising in the workplace); Marx, supra note 53, at 30 (quoting Karen Nussbaum, Executive Director of 9to5, National Association of Working Women: "Not only are employees rejecting surveillance techniques, but the courts are too. Legal challenges to employer access to databases of personal information are expected to grow. And workers are filing privacy suits against their employers in unprecedented numbers."). See generally Mark E. Brossman, Workers Gain Privacy Rights by Legislation, Judicial Action, NAT'L L.J., April 9, 1990, at 28 (discussing the change from a legal climate in which employers could monitor employees with impunity to a climate limiting that authority substantially, and also summarizing the various statutory and common law bases for those limitations upon employer authority).

132. IRA M. SHEPARD, WORKPLACE PRIVACY: EMPLOYEE TESTING, SURVEILLANCE, WRONGFUL DISCHARGE, AND OTHER AREAS OF VULNERABILITY 1-2 (2d ed. 1989). As stated in that report:

The increasing occurrence of medium to high six-figure damage awards in employment litigation, which is reflected in these survey results, has fueled the flames of employee privacy litigation. The movement into the high tech age of computer analysis and supervision of employees will inevitably fan these flames and increase the workplace privacy issues that may be addressed by the courts and legislatures.

\textit{Id.} at 2. The report refers to a survey of workplace-privacy jury verdicts that illustrates "the dramatic increase in workplace privacy cases filed in the 1980s and the astronomical increase in average jury verdicts against employers in workplace-privacy cases since 1985." \textit{Id.} at 1. By contrast to the 1979-1980 period, in which there were no reported workplace-privacy jury verdicts, the average verdict in the period 1985-1987 was $316,000. \textit{Id.} at 1-2. Further, the number of reported jury verdicts against employers in cases of that type increased twenty-fold from the period 1981-1984 to the period 1985-1987. \textit{Id.} at 2. The second edition of Shepard's book describes a new survey by the same firm concerning these trends. The new survey found that 72\% of workplace-privacy trials between 1985 and 1988 were won by the employee, with an average award of $375,307 and a median of $97,000. \textit{Id.}

133. \textit{See THE ELECTRONIC SUPERVISOR, supra note 6, at 97-100 (summarizing the positive and negative implications of increased monitoring).}

134. "[I]n the past, the economics of monitoring tended to work against intensive mass surveillance. But technological breakthroughs have greatly reduced the cost of monitoring." Marx & Sherizen, supra note 26, at 62.

135. \textit{See supra} note 120 (stating that only 12\% of United States workers are unionized).
employees," the likely outcome of balancing the pros and cons of monitoring and surveillance seems quite clear. We may anticipate a substantially increased use of artificial monitoring and surveillance in the workplace in the near future.

E. Distinguishing Artificial Monitoring and Surveillance from Direct Human Supervision—The Modern Panoptican

It may be argued that all these techniques amount to nothing more than high-technology methods of allowing the employer to engage in activity in which employers always have been appropriately engaged. In other words, this technology simply allows employers to observe employees in the performance of their work.

Furthermore, it may be argued that the existence of "Panoptican" monitoring and surveillance in the workplace is hardly a new development, particularly in the workplace, and that it has withstood the test of time in the absence of restrictive legislation. Frederick W. Taylor, commonly referred to as the father of scientific management, began his studies of the management of work in the 1880s. Taylor's scientific management concepts, which included aspects of efficiency and monitoring, were incorporated rapidly by American industry. An example is the assembly line production process established...

136. See Piturro, supra note 95, at 32.
137. N. Faye Angel, Evaluating Employees by Computer—Reasons To Appraise Employee Performance Electronically, PERSONNEL ADMIN., Nov. 1989, at 67. For example, some experts claim that as many as 30 million visual display terminal users might have their work monitored electronically by the year 2000. Id.
138. See Marx & Sherizen, supra note 26, at 62 (recognizing in a discussion of the differences between personal observation and artificial monitoring and surveillance that it has always been the job of a supervisor to watch his subordinates); Columbia Professor Contends Monitoring Does Not Breach Employee Privacy Rights, Daily Lab. Rep. (BNA) No. 44, at A-7 (March 8, 1989) (reporting the views of renowned privacy expert Alan F. Westin to be that electronic monitoring is not fundamentally different from traditional supervision and opposing then-pending legislative proposals to regulate that activity).
139. Gary L. Davis, Note, Electronic Surveillance and the Right of Privacy, 27 MONT. L. REV. 173, 173 (1966). The author points out that wiretapping began shortly after the telegraph was invented. Id.
140. See Danaan, supra note 75, at 1. The term Panoptican is derived from the work of Jeremy Bentham at the turn of the 19th century. He developed the concept of a polygonal structure known as the Panopticon for use by the British government as a prison factory. This building, which the government ultimately decided not to build, would have utilized a central tower from which rows of glass walls would emanate. Mirrors affixed to the tower would have enabled the supervisors to observe the inhabitants of the glass cells, but those supervisors would not have been observable by the inhabitants. Marx, supra note 53, at 22 (comments of Shoshana Zuboff, associate professor at the Harvard Business School). Inasmuch as the device was designed to be continuous and automatic, it was theorized that it would "ensure desirable conduct." Gandy, supra note 7, at 63.
141. Richard E. Walton, From Control to Commitment in the Workplace, HARV. BUS. REV., Mar./Apr. 1985, at 76.
lished by Ford Motor Company in 1903. The early applications of monitoring were often quite pervasive; in fact, they were not necessarily limited to measurement of the employee's work performance. The monitoring and surveillance frequently extended to very private aspects of the employee's personal life.

It also may be argued that artificial monitoring and surveillance does not take place only in the workplace in modern society and that, as a result of the dizzying pace of modern technological developments affecting all aspects of our lives, most of us simply expect and accept this activity. All of us do expect to be watched artificially in the course of our daily lives. We voluntarily enter into many situations in which we assume that our activities will be artificially observed. For example, we know that banks are commonly robbed and we (excluding those with felony in their hearts) rarely object to the omnipresent camera pointed at us from the ceiling in the bank lobby or from the inside of the automatic teller machine. In fact, we might well be disturbed to find that it did not exist because of the protection that the camera provides. On the other hand, we expect monitoring to be limited to observations reasonably necessary to accomplish that protection. For example, we might well feel that our privacy had been invaded if video surveillance extended to the bank washroom. Also, the workplace is inherently different because of the amount of time that most of us spend there and the lack of practical options for most of us not to be there.

Despite this ordinary expectation of the existence of monitoring and surveillance and its historical pervasiveness in the workplace, the pace of technological development has significantly altered the nature of this artificial monitoring. In many cases in which the newer methods are utilized, it is not possible to detect the presence of the observer. Detected or not, that observer may well be a person who has no direct contact with or concern for the person being observed. The observation is likely more pervasive in the sense that it is often continuous and automatic. Once the results of the observation are collected, the technology allows for automatic analysis of the information in ways not possible before. For example, the new information can be matched

142. The Electronic Supervisor, supra note 6, at 18.
143. Id. at 19.
144. See Laplante, supra note 85, at 58. LaPlante states, "In George Orwell's 1984, there is no question that Big Brother is there, always watching, always listening. Indeed, it would be hard for any inhabitant of that world to be unaware of that fact." Id.
145. See Gandy, supra note 7, at 63 (pointing out that information may be processed by "unknown and faceless technicians and specialists" without any personal interest in the outcome); Marx & Sherizen, supra note 26, at 62 (pointing out that the small physical size of much of the hardware and the ability of the user to activate it from distant locations makes it different from personal observation).
146. Gandy, supra note 7, at 63.
147. Id. at 64; Marx & Sherizen, supra note 26, at 65 (noting that artificial monitoring and surveillance can be "omnipresent and tireless").
by computer with information from other sources.148 These analytical methods then allow the observer to generate information not only revealing what the observed person did, but what they have the potential to do in the future.149 Finally, the instruments necessary to conduct the monitoring or surveillance now are available to a far greater number of people, and it is easier to rapidly disseminate the results of the monitoring or surveillance to third parties. In sum, the sophistication of the techniques increases their potential dangerousness to privacy.

One final factor must be taken into account in contrasting the current scenario to the past. Private business plays an increasingly powerful role in the lives of Americans. As stated in a recent news article:

It has been 17 years since Congress passed the Privacy Act of 1974, which restricts Government agencies from exchanging information, regulates the information that agencies may collect and gives citizens rights to inspect their files. But the act doesn't apply to businesses. With the development of increasingly powerful computer and communications technologies, some experts say, corporations may pose a greater threat to privacy than does big government.150

Many Americans are apparently more fearful of their employer than the government.181 Employee awareness and fear of employer monitoring and surveillance will grow as the impact of such monitoring is increasingly felt by the American worker.

F. Impact of Artificial Monitoring and Surveillance on Employees

The actual effects of this increasingly pervasive monitoring and surveillance in the workplace are not yet clear. A number of studies are currently underway to determine those effects.182 Additionally, there are conflicting opinions about worker attitudes concerning monitoring and surveillance. A recent study drew a distinction between surveillance and computer based monitoring in examining worker attitudes.183 The study concluded that many employees object to surveillance but a relatively small percentage object to monitoring.

Many articles in the trade and popular press claim or imply that most workers oppose the practice of monitoring. Our survey results do not support such claims . . . "Electronic surveillance" uses audio and visual equipment to examine employee behaviors and personal characteristics. About 52 percent of survey respondents agreed to some extent that all electronic surveil-
lance should be illegal. This compares to 30.5 percent agreeing with the statement that monitoring should be illegal. Thus, employees did differentiate between surveillance and computer monitoring. This is an important distinction. Trade and popular press articles have discussed cases of pervasive monitor designs that incorporated video or audio taping. The fact that these monitors included surveillance, rather than that they monitored work, may be at the root of the vocal opposition to their use.

Although the actual effects are uncertain, the potential effects may be categorized into three often overlapping groups: (1) quality of the employee’s life, (2) the employee’s right to privacy, and (3) fairness to the employee.

1. Quality of Employee’s Life

Monitoring and surveillance may cause an unusual incidence of stress and stress-related illnesses, both physical and psychological. A report issued by the Office of Technology Assessment emphasizes that the scientific evidence bearing on this potential side effect is not conclusive. As a result of this uncertainty, the National Institute for Occupational Safety and Health is planning to undertake a study, to be completed in 1992, examining the stress and performance effects of the use of electronic monitoring to set workplace performance standards.

Furthermore, artificial monitoring and surveillance has the capacity to eliminate worker autonomy. In other words, the ability of the worker to decide how his job will be done is severely impaired. Why is this an important consideration?

154. Id.; see also Gozner, supra note 74, at C1 (reporting the Grant & Higgins study as well as a survey by Louis Harris & Associates for Equifax in which most respondents indicated a belief that some form of workplace monitoring is necessary).

155. See Danaan, supra note 75, at 4 (reporting that both the fact of monitoring and the use of the resulting information are stress-creating events); Ronald E. Roe, Injured by Big Brother?: Study Shows Monitored Workers Get Hurt More, Newsday, Oct. 5, 1990, at 49 (reporting a study by a major telecommunications union and an ergonomics expert that concluded that employees monitored qualitatively and quantitatively suffer a higher incidence of psychological ailments and repetitive strain injuries); Frank Swoboda, Study Links Electronic Monitoring, Stress, Wash. Post, Oct. 14, 1990, at H3 (reporting a study conducted by the University of Wisconsin for the Communication Workers of America, based on a random group of workers from regional telephone companies, which concluded that workers whose job performances are monitored by computer suffer more from job-related stress than those not monitored in this manner). See generally Jonathan Peterson, New Job Pressures Take Human Toll, Wash. Post, July 15, 1990, at H3 (reporting on the “skyrocketing” stress claims arising from a multitude of modern job pressures, including electronic monitoring and surveillance); Jonathan Peterson, Feeling Tense? You’re Probably Doing Your Job; Stress: As Competition Grows, So Do Workplace Tensions, from Boardroom to Shop Floor, Everyone Frets, L.A. Times, Apr. 29, 1990, at D1 (reporting the multitude of factors causing stress in the modern workplace, including monitoring and surveillance).

156. The Electronic Supervisor, supra note 6, at 50-55.


158. See The Electronic Supervisor, supra note 6, at 8.
Control over personal information is particularly important for our sense of self. When an individual's room, pocketbook, or body can be searched at will, when conversations and even thoughts are available for instant inspection by outsiders, openness and honesty lose their value. Distrust becomes institutionalized and an important and even sacred element of the social bond is damaged.\(^{106}\)

Corresponding to the loss of a feeling of autonomy is the possibility that there will be a reduction in the level of trust in the employer-employee relationship because the employee feels "spied upon."\(^{160}\) It has the capacity to make the employee believe that their employer's basic assumption about them is that they are unproductive or dishonest and that they must struggle to overcome that assumption. In a 1990 telephone conversation with the legislative director for the Communications Workers of America, Lou Gerber, he told me that many employers seem to live by the motto "In God we trust. Others we monitor."\(^{161}\)

All of these detrimental effects have potentially serious consequences for American society as a whole. Although the simple desire of employees to maintain an acceptable quality of life is certainly an important factor, Congress and the courts must also consider the reality that failure to maintain that quality of life is likely to translate into higher costs to society as a whole, such as decreased product quality and increased burdens on our already overtaxed health care system.

2. Privacy: "The Right 'to Be Let Alone'"\(^{162}\)

Employees may object to the ability of employers to observe their "private" behavior. It may, of course, be argued that artificial monitoring and surveillance in the workplace is not really an issue of privacy because employees expect to be observed as part of the normal supervision process; employees do not have a reasonable expectation of privacy in the employment relationship. It is in fact true that an employee impliedly consents by voluntarily entering into the employment relationship to be subjected to a certain level of supervision. If the level of monitoring and surveillance exceeds that which the ordinary employee would impliedly accept by taking a job, the employer may then expressly require consent as a condition of extending a job offer. As discussed below, these factors do render most common law concepts of privacy an inadequate solution to the problems associated with artificial monitoring and surveillance in the workplace. And they do not render the employee's privacy concerns less important in an inquiry into the design of an appropriate legal

159. See Marx & Sherizen, supra note 26, at 62.
160. See DANAAN, supra note 75, at 5.
161. Telephone Interview with Lou Gerber, Legislative Director, Communications Workers of America (July 3, 1990).
solution to this problem. The nature of the employer-employee bargaining relationship is such that many, if not most, United States employees do not possess the luxury of simply refusing to enter into the employment relationship when they learn that intrusive monitoring and surveillance will be one of its key elements.

Privacy issues of this nature are a significant and growing concern for Americans. The above-discussed Equifax report indicates that 79% of Americans now say that they are very concerned or somewhat concerned about threats to personal privacy in America today.\textsuperscript{163} This reflects a significant increase from the level of concern expressed in a similar 1978 study\textsuperscript{164} and a small increase over a similar 1983 study.\textsuperscript{165} The Equifax study indicates that a rising percentage of Americans, 30% now as opposed to 14% in 1978, have decided not to apply for a job, credit, or insurance because they did not want to disclose certain personal information.\textsuperscript{166}

Why might an employee have privacy concerns about artificial monitoring and surveillance? One factor is the above-discussed desire for personal autonomy. Another factor is the possibility that artificial monitoring or surveillance will generate information about an employee that could be used for impermissible purposes, such as identifying and disciplining whistleblowers. Similarly, the employee may be concerned that the information generated will be used in a manner that is unfair. Finally, the possibility exists of inappropriate transmission of the information to third parties other than the employer.

Why do these privacy interests in the workplace deserve protection by our legal system? The reason lies in the fact that American society values and thrives on the diversity of its citizenry. To the extent that individual citizens do not have the right to decide which aspects of their personal lives are to remain known to them alone, we are in danger of losing that diversity. The likelihood that individuals will develop their individual and unique characteristics will be diminished and American society will be less diverse, creating a less satisfying way of life and a less productive economy.

3. Fairness

A part of the concern of any employee about workplace privacy may be grounded in the fact that the potential for basic unfairness is significant when artificial monitoring and surveillance techniques are used. In other words, the potential exists that employee performance will be evaluated in a manner that does not truly measure that employee's value to the organization. For example, these techniques may focus on the employee's weak points, failing to observe the employee's strong points. The employee's pace of work may be accelerated

\textsuperscript{163} THE EQUIFAX REPORT, supra note 105, at 2 (96% are very concerned while 33% are somewhat concerned).
\textsuperscript{164} Id.
\textsuperscript{165} Id.
\textsuperscript{166} Id. at 14.
to a level that, although attainable on occasion, is unacceptably high on a sustained basis. Errors in measurement may occur that the employee cannot effectively refute because of the nature of the testing. Some employees may find ways to "game" the system, resulting in incorrect input and adversely affecting those who do not "game" the system. The focus may be strictly on quantity, ignoring the quality factor. Further, an individual supervisor may be able to manipulate the system to adversely affect an individual worker against whom he holds a grudge. As a result of these factors, employees are generally more willing to accept monitoring when they are granted a role in determining the manner in which it is implemented in the workplace.

Despite these potential negative effects of artificial monitoring and surveillance in the areas of quality of life, privacy, and fairness, even critics of monitoring and surveillance techniques agree that it has potentially positive effects. In addition, the critics also acknowledge that many of the negative potential effects upon employees can be reduced or eliminated through the use of some common-sense management guidelines. Techniques to reduce the potentially negative effects of artificial monitoring and surveillance include (1) letting employees know in advance about the monitoring or surveillance; (2) not using subliminal messages; (3) evaluating only relevant activity; (4) collecting results by groups of workers, not individuals; (5) using factors other than the results of monitoring and surveillance in setting performance standards; and (6) making sure that those standards allow for variables that the specific monitoring system does not measure.

Finally, artificial monitoring and surveillance techniques may well be physically less intrusive than other forms of monitoring and surveillance. They can be used to provide a safer workplace, to judge the performance of employees objectively and fairly, and to protect employees against false accusations.

In other words, the potential negative effects of monitoring and surveillance do not argue for its prohibition. Instead, they argue for its regulation in a manner that assures it will be used fairly and will not adversely affect the quality of the worker's life or her right to personal autonomy.

167. See Kilborn, supra note 20.

168. See, e.g., THE ELECTRONIC SUPERVISOR, supra note 6, at 38-40.

169. See, e.g., Holloway McCandless, Computer Monitoring: Is It "Big Brother" Watching: Manager's Shoptalk, WORKING WOMAN, Nov. 1988, at 38; see also Angel, supra note 137, at 67 (discussing the key elements in a successful computer monitoring system: reasonable work standards, appraisal of relevant work only, evaluation at fair and regular time intervals, and employee access to monitoring records).

170. See Marx & Sherizen, supra note 26, at 62.

III. An Overview of Current Legal Limitations on the Use of Artificial Monitoring and Surveillance by Employers in the Private Sector

Assume that our hypothetical human resource director is ultimately terminated from her latest position. She was undergoing extreme stress, caused at least in part by discovering the full extent of her employer's monitoring and surveillance policies. Her supervisor then determined that many of her personnel decisions were neither soundly based nor adequately documented. She believes that many of her decisions were reviewed out of context and therefore were not representative samples, and she also believes that some of her decisions were affected by the stressful working conditions. Do constitutional and statutory privacy protections offer her a legal remedy? Probably not. Could the problem have been avoided in the first instance? Probably yes.

A. Constitutional and Statutory Limitations

Although there have been recent proposals to amend the United States Constitution to expand privacy guarantees, the Constitution does not generally limit monitoring and surveillance in private sector workplaces. The simple absence of state action generally renders the Fourth Amendment protection against unreasonable searches and seizures inapplicable. As a result, public employees for the most part have significantly greater protection than employees in the private sector. Potentially, private employers, who are generally

172. There have been recent proposals to amend the United States Constitution by adding a Twenty-Seventh Amendment to specify, among other things, that the guarantee in the Fourth Amendment against unreasonable searches applies regardless of the form of the technological method employed. See Fickel, supra note 1, at 54. Even if the Constitution were expanded in that manner, action taken by a private employer against its employee would not, as a general rule, violate the constitutional rights of the employee because of the absence of state action. By contrast, if a government employee is monitored by the government, the employee may potentially have a claim that his constitutional rights have been violated. In addition, although the Privacy Act of 1974, 5 U.S.C. § 552a (1988), applies primarily to records maintained by the federal government, it does apply to certain government contractors. See generally Office of Technology Assessment, U.S. Congress, Pub. No. 296, Electronic Record Systems and Individual Technology (1986) (concluding that the federal government is not adequately monitoring Privacy Act compliance).

173. See Decker, supra note 36, at 108 (discussing the various sources of the right of privacy in the Constitution and pointing out that "almost no private sector employer is bound by these constitutional privacy restraints"); Martin N. Flics, Comment, Employee Privacy Rights: A Proposal, 47 Fordham L. Rev., 155, 159-64 (1978); Furfaro & Josephson, supra note 1, at 3 n.1 (pointing out that the Supreme Court has interpreted this state action requirement "conservatively"); Note supra note 18, at 1906 ("Federal Constitutional privacy claims, available only to public employees, have not been extended to protect workers from monitoring.") (citations omitted)). Note also that federal employees receive in addition to the protections provided by the Constitution, statutory protections not generally applicable to private sector employees. For example, the Civil Service Reform Act of 1978 protects federal employees who disclose certain information concerning criminal or other behavior of fellow employees. 5 U.S.C. § 2302(b)(8) (1988).

174. Protections against intrusions on privacy are provided by many foreign countries. See
not limited by the Constitution, are a greater threat to the privacy of individuals than the government.

Cases interpreting the application of these constitutional protections to government employees are discussed below because they are relevant, by analogy, to the determination of whether private sector employees have a reasonable expectation of privacy in the workplace. That inquiry concerning reasonableness is central to common law privacy claims as well as Fourth Amendment claims by government workers.

In addition to the protection given to government workers by the Constitution, a number of states have privacy guarantees in their own constitutions. Additionally, violation of privacy is, in certain limited circumstances, a violation of state criminal statutes.

Although the United States and state constitutions do not ordinarily limit artificial monitoring and surveillance activity by private employers, there is a plethora of federal and state protections from artificial monitoring and surveillance, but only in certain limited circumstances. A significant portion of employee protections is created by state statutes. In some cases, federal law may have a preemptive effect. In other cases, the state statute may be expressly or impliedly the exclusive remedy of the employee for the particular alleged violation.

Markoff, supra note 50, at 7.

175. Infra part III.B.2.a.

176. See Decker, supra note 36, at 130 n.254; 2 Joseph D. Levesque, People in Organizations Series: Managing Employee Privacy Rights and Wrongful Discharge Problems II.1.8 to II.1.9 (1989) (listing state constitutional and statutory provisions about privacy); Shepard, supra note 132, at 30-32; Robert E. Smith, Compilation of State and Federal Privacy Laws 1984-85, at 28-29 (1984) (listing various state and federal laws concerning privacy statutes). As a general rule, these state constitutional provisions are interpreted consistently with the privacy guarantee under the United States Constitution in that they only limit the action of government employers. See, e.g., Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123 (Alaska 1989) (holding that the Alaska Constitution's guarantee of the right to privacy is not applicable to the actions of private parties). But see Porten v. University of San Francisco, 134 Cal. Rptr. 839 (Cal. Ct. App. 1976) (extending California Constitution's guarantee of privacy to private employees); Wilkinson v. Times Mirror Corp., 264 Cal. Rptr. 194, 200 (Cal. Ct. App. 1989) (holding government action is not required to trigger state constitutional guarantee of privacy). Although the employee drug testing program involved in Wilkinson was upheld, the court stated:

Common experience with the ever-increasing use of computers in contemporary society confirms that the amendment was needed and intended to safeguard individual privacy from intrusion by both private and governmental action. That common experience makes it only too evident that personal privacy is threatened by the information-gathering capabilities and activities not just of government, but of private business as well. If the right of privacy is to exist as more than a memory or dream, the power of both public and private institutions to collect and preserve data about individual citizens must be subject to constitutional control.

Id.

177. 2 Levesque, supra note 176, at II.1.11 (listing four areas of invasion of privacy that create a cause of action under certain state statutes).


179. Id. at 99.
The federal and state statutes are discussed below, but not in an attempt to provide a comprehensive analysis of all provisions presented. Instead, the purpose is to demonstrate that these provisions, viewed in their entirety, do not provide a comprehensive solution to the problems addressed by this Article.

1. **Occupational Safety and Health Act and Similar State Statutes**

Worker safety laws alone do not provide a comprehensive solution to the problems associated with artificial monitoring and surveillance in the workplace. First, they do not provide for advance employee notice or opportunity to inspect records. Second, they generally have ignored long-term stress as a safety factor.

The Occupational Safety and Health Act of 1970 ("OSHA") could, in limited circumstances, restrict particular employer monitoring and surveillance practices. For example, it is conceivable that scientific studies will at some point in the future irrefutably establish that video display terminals used in the monitoring and surveillance process pose a serious health hazard. OSHA mandates that each employer provide each employee with a place of employment free from "recognized hazards that are causing or are likely to cause death or serious physical harm." Based on current research, however, it is unlikely that the common artificial monitoring and surveillance devices discussed above would fall into this category except in the most unusual of circumstances.

OSHA does, in fact, recognize the possibility of psychological damage from workplace conditions. But the statutory mandate to employers concerning workplace safety ordinarily would not apply, either because the hazard is not one that is recognized or because the type of damage it is likely to cause is not

180. See, e.g., The Occupational Safety and Health Act, 29 U.S.C. § 657(a)(3) (1988) ("OSHA"). OSHA provides employees with the opportunity to inspect records in limited circumstances. Id. However, this limited opportunity to inspect does not provide employees with significant protection from the myriad forms of monitoring and surveillance available to employers.

181. Id. § 652(a)(6).

182. Id. §§ 651-78.

183. Id. § 652(5) (defining "employer" as any person with employees engaged in a business affecting interstate commerce, excluding federal and state government).

184. Id. § 652(a)(6).

185. Id. § 654(a)(1). Note also that OSHA requires employers to disclose certain medical records about their employees to the federal government upon demand. Id. § 657(c)(2)-(3); see also 29 C.F.R. § 1910.20 (1991) (discussing access to employee exposure and medical records).

186. The congressional statement of purpose notes that the Act is to foster research in the field of occupational health and safety, "including psychological factors involved." 29 U.S.C. § 651(b)(5). In fact, the National Institute for Occupational Safety and Health is currently conducting research, as discussed above, concerning the relationship between stress and artificial monitoring and surveillance in the workplace. See Robert A. Bohrer, Fear and Trembling in the Twentieth Century: Technological Risk, Uncertainty and Emotional Distress, 1984 Wis. L. Rev. 83, 120 n.168 ("Although OSHA has not, to date, considered in any systematic way the problem of workplace-induced psychological stress, that problem has begun to attract considerable attention in the closely related context of worker's compensation law." (citations omitted)).
"death or physical harm."  

Many states and some municipalities have enacted legislation regulating health and safety in the workplace in a manner similar to OSHA. For example, the question of the long-term health effects of video display terminals ("VDT's") upon employees is currently a matter of significant debate. A significant amount of attention in the popular press has been given to an ordinance enacted by the city of San Francisco placing restrictions upon the use of VDTs in the private workplace.

2. State Worker's Compensation Statutes

In a manner similar to workers' safety laws, workers' compensation laws are an inadequate remedy for the problem of monitoring and surveillance because of their emphasis on physical injury and injury caused by sudden events. The states are currently split on the question of whether to permit recovery of monitoring-induced stress. Most states, however, will not permit any recovery under this theory unless the stress can be characterized as "unusual."

3. Antidiscrimination in Employment Legislation

Various statutes prohibiting employment discrimination would provide relief from artificial monitoring and surveillance in the workplace when it is used for illegitimate purposes, for instance as a tool to hide discrimination on an improper basis. Those statutes are not, however, a protection in most cases when the artificial techniques are being used for legitimate reasons.

Title VII of the Civil Rights Act of 1964, for example, prohibits employ-

---

187. 29 U.S.C. § 654(a)(1) (stating the central mandate of OSHA—that every employer must provide a workplace "free from recognized hazards that are causing or are likely to cause death or serious physical harm" to employees).
189. See San Francisco Mayor Signs Revolutionary VDT Ordinance; Mayor Art Agnos Moni-
tor, PC WK., Jan. 7, 1991, at 137 (reporting that these restrictions apply only to employers with 15 or more employees and that, after a four-year phase-in period, employers will be required to provide detachable keyboards, height-adjustable monitors, adequate lighting, and breaks).
191. The Electronic Supervisor, supra note 6, at 111-12.
ARTIFICIAL MONITORING OF EMPLOYEES

ment discrimination based on race, color, religion, sex, or national origin. Employee monitoring and surveillance techniques that are used to discriminate intentionally or that have a disparate impact on members of a protected class might give rise to a Title VII claim. A similar claim might arise under other federal statutes that, correspondingly, prohibit employment discrimination for various other reasons. For example, the Age Discrimination in Employment Act of 1967 prohibits employment discrimination on the basis of age, and section 503 of the Rehabilitation Act of 1973 prohibits certain discrimination in employment by certain federal contractors on the basis of a recognized handicap. Recently, the Americans With Disabilities Act became law. Title I of that new law, which will take effect for employers with twenty-five or more employees on July 26, 1992, and on July 26, 1994, for employers with fifteen to twenty-four employees, vastly expands the prohibitions against employment discrimination on the basis of disabilities. In addi-


193. Griggs v. Duke Power Co., 401 U.S. 424 (1971) (holding that a facially neutral employment policy violates Title VII if discriminatory in effect); see, e.g., Johnson v. Pike Corp., 332 F. Supp. 490 (C.D. Cal. 1971) (holding that discharging employees whose wages had been garnished violated the 1964 Civil Rights Act because of the discriminatory impact on members of minority groups); Gregory v. Litton Sys., Inc., 316 F. Supp. 401 (C.D. Cal. 1970), modified, 472 F.2d 631 (9th Cir. 1972) (holding that use by the employer of information about arrests, not convictions, for a number of offenses other than minor offenses was impermissible). See generally Pamela L. Perry, Two Faces of Disparate Impact Discrimination, 59 FORDHAM L. REV. 523 (1991) (discussing the differences between the "fault theory" of disparate impact and the "effects theory," the latter of which was generally adopted by the Civil Rights Act of 1991); Russell J. Davis, Annotation, Employer's Consideration of Background or "Character" Investigation of Applicant for Employment, Including Inquiry into Credit Record, Military Service Record, and the Like, as Unlawful Employment Practice Violative of Title VII of Civil Rights Act of 1964, as Amended (42 USCS secs. 2000e et seq.), 40 A.L.R. FED. 473 (1978); Annotation, Consideration of Arrest Record as Unlawful Employment Practice Violative of Title VII of Civil Rights Act of 1964 (42 USCS secs. 2000e et seq.), 33 A.L.R. FED. 263 (1977).


195. 29 U.S.C. § 793 (1988); see, e.g., Davis v. Bucher, 451 F. Supp. 791 (E.D. Pa. 1978) (holding that a blanket policy prohibiting employment of former drug addicts was violation of the 1973 Rehabilitation Act). Note also that certain employers covered by this statute or by the Vietnam Era Readjustment Act, 38 U.S.C. § 2012 (1988), are limited in the disclosure of medical information concerning employees. See Leckelt v. Board of Comm'rs, 909 F.2d 820 (5th Cir. 1990) (upholding the dismissal of suit brought by former nurse against local government hospital claiming that his discharge for failure to submit to his employer results of an HIV antibody test violated his rights under section 504 of the Rehabilitation Act of 1973, as well as under various other state and federal laws).


197. Id. §§ 12111-12117.

198. See Novack, supra note 34, at 98. Novack, referring to the development of medical databases by employers to control medical expenses and inquiries asks, "Will employers use the data they are accumulating to weed out less healthy workers and malingerers?" Id. He concludes:
tion to the provisions of this new law generally prohibiting employment discrimination on the basis of disability, it will severely curtail the use of medical examinations by employers. Similarly, many states limit the use of tests by private employers to determine whether an employee is infected with or is a carrier of a communicable disease.

In addition to these federal statutes, which are generally labeled as antidiscrimination-in-employment laws, other federal statutes, such as OSHA, contain anti retaliation provisions designed to protect employees against adverse personnel decisions based on the exercise of federally created employee rights. For example, both Title VII and OSHA prohibit retaliation against an employee for exercising her rights under those laws. Other federal statutes protect employees from adverse personnel decisions based on their exercise of other rights that are not necessarily related to the employment relationship. For example, the right of an employer to discharge an employee because of wage garnishments is limited by the Consumer Credit Protection Act.

For better or worse, they can't. In July 1992 the Americans With Disabilities Act, passed last year, will come into force, making it illegal for employers to refuse to hire people who have had health problems. The law might well also bar employers from rejecting people because they filed worker compensation claims.


199. 42 U.S.C. § 12112 (c). Final regulations under the Americans With Disabilities Act were adopted by the Equal Employment Opportunity Commission on July 26, 1991. 29 C.F.R. § 1630 (1991). These regulations specifically prohibit employment tests or other selection criteria that screen out or tend to screen out individuals with disabilities unless a job-related business necessity is established. Id. § 1630.10. In the case of medical examinations, these are permissible after an employment offer is made (even if the offer is conditional on the outcome of the test) if all employees in that same job category are subjected to the test. Id. § 1630.14(b). Such exams may not be used to screen out disabled persons for reasons that are not justified by a job-related business necessity. Id. § 1630.14(b)(3). Employees may also be required to take a medical examination. Id. § 1630.14(c).

200. See SHEPARD, supra note 132, at 166 (pointing out that some states expressly limit the right of employers to administer blood tests to detect the presence of HIV antibodies while other states have laws prohibiting handicap discrimination that may limit that right); DECKER, supra note 36, at 94-95 (pointing out that testing is required for certain occupations and prohibited in other circumstances by various state laws).


ARTIFICIAL MONITORING OF EMPLOYEES

Many states have antidiscrimination-in-employment statutes that, in a manner similar to Title VII, prohibit discrimination in employment based on race, color, religion, sex, or national origin. Similarly, many state statutes outlaw employment discrimination based on handicap. Some states specifically prohibit discrimination in employment based upon genetic testing results. A substantial number of states prohibit lifestyle discrimination and at least one state is considering a law to prevent discrimination against off-duty smokers.

In a manner similar to the federal statutes discussed above, it is not uncommon for state statutes to protect employees against retaliation for the exercise of state-created employment rights. Nor is it uncommon for state statutes to protect employees against retaliation for the exercise of other state-created rights not necessarily related to the employment relationship. But, like the federal statutes, state statutes in this area do not prohibit the use of monitoring or surveillance techniques, except where such techniques are used to retaliate against employees.

4. National Labor Relations Act and Similar State Labor Statutes

Reliance on federal and state labor laws and the collective bargaining process is not the long-term solution to the problems of artificial monitoring and surveillance in the workplace. Due primarily to the small and declining percentage of unionized workers, this simply would not provide a comprehensive solution to the problem. The National Labor Relations Act ("NLRA") does not prohibit the use of artificial monitoring and surveillance. Similarly, that activity ordinarily would not be expressly prohibited in the states statutes similar to NLRA.

Despite the absence of an express prohibition, artificial monitoring and surveillance may well violate the prohibition in NLRA against employer activities designed to prevent employees from exercising their rights under the federal labor law. Furthermore, it is possible that artificial monitoring and surveil-

Bankruptcy Code or because of association with debtor).

203. Decker, supra note 36, at 82 n.418.
204. Id. at 83 nn.420-23.
205. See Swoboda, supra note 61, at H3 (describing New Jersey statute prohibiting employment discrimination based upon "atypical hereditary cellular or blood trait").
206. See Stop Bosses' Invasion of Workers' Privacy, supra note 69, at 6A (reporting that Colorado, Kentucky, Oregon, Rhode Island, South Carolina, Tennessee, and Virginia all have statutes banning employment discrimination based on lifestyle).
207. See Mauro & Lawlor, supra note 36, at 1A.
208. See Decker, supra note 36, at 86 n.443 (discussing the state whistleblowing statutes).
209. See supra notes 119-20 and accompanying text (discussing the decrease in the number of unionized workers in the United States).
211. See Decker, supra note 36, at 81 nn.408-09.
212. 29 U.S.C. § 158(a)(1) (making it an unfair labor practice for an employer to restrain or coerce employees in the exercise of their rights under NLRA); see, e.g., NLRB v. J. Weingarten,
lance would violate the terms of a collective bargaining agreement under certain circumstances. As discussed above, the relatively small unionized port-

Inc., 420 U.S. 251 (1975) (holding that employer violated section 8(a)(1) of NLRA by denying an employee's request for union presence at investigatory interview to determine whether disciplinary action should be taken against the employee for theft). Compare NLRB v. R.C. Mahon Co., 269 F.2d 44 (6th Cir. 1959) (holding that employer observations of employee activities carried out in employer's plant on company time was not violation of NLRA section 8(a)(1), even in absence of company rule permitting such observation) with Stone & Webster Eng'g Corp. v. NLRB, 536 F.2d 461 (1st Cir. 1976) (holding that employer's surveillance of union organizer's attempts to use pay telephone at plant was violation of section 8(a)(1)).

Arguments of this nature have often arisen in labor-arbitrations decisions involving searches of employees. For example, one arbitration involved the employer's insistence that it be allowed to search the lunch box of an employee suspected of conducting gambling activities on the employer's premises. The arbitrator ruled that the fact the employees were asked to purchase their own locks for tool boxes gave those employees a "half-private" and "half-company" property characterization, with the result that the employer could not search the boxes at any time for any reason. However, the arbitrator found that the employer had a reasonable basis in this particular situation. In re Kawneer Co., 86 Lab. Arb. (BNA) 297 (Dec. 27, 1985) (Alexander, Arb.).

In re Boone Energy, 85 Lab. Arb. (BNA) 27 (July 2, 1985) (O'Connell, Arb.), the employer observed a nonclassified employee under the influence of a controlled substance and used that observation as the primary basis to conduct a search of all employees. The employer required the workers to submit blood and urine samples and to sign an authorization sheet. The arbitrator ruled that the employer could search for contraband in this manner as long as it was done in a nondiscriminatory fashion, but the employer could not use a positive blood or urine test to conclusively determine that the employee was under the influence of controlled substances while working. Id.; see also In re Daniel Int'l Corp., 83 Lab. Arb. (BNA) 109 (Nov. 20, 1984) (Thornell, Arb.) (halving back pay when employee refused to submit to second lunch box search upon entering nuclear power plant was too severe a punishment); In re Lake Park, 83 Lab. Arb. (BNA) 27 (July 6, 1984) (Griffin, Arb.) (discharge of food service worker who refused to allow inspection of purse at end of shift was proper when done in response to reports of incidents of theft on employer's premises). See generally Charles B. Craver, The Inquisitorial Process in Private Employment, 63 CORNELL L. REV. 1, 61-63 (1977) (discussing partial restrictions on use of surveillance techniques by employers under NLRA).

213. See, e.g., In re Eico, Inc., 44 Lab. Arb. (BNA) 563 (Apr. 14, 1965) (Delaney, Arb.). In Eico, the employer installed and operated a closed circuit television system on the production floor in one of its plants. Although there were 19 floor supervisors, this system allowed the plant manager to maintain continual video surveillance in the plant manager's office. The union claimed that this surveillance was a violation of the right to privacy; that it was illegal "spying"; and that it violated the collective bargaining agreement, which required the employer to continue in force any "conditions of employment which are not covered by this agreement which are beneficial to employees." Id. at 564. The arbitrator's favorable ruling for the union was based solely on the contractual argument. The arbitrator found that the surveillance imposed an "appreciable and intolerable" burden on employees, stating:

The device at hand is not only personally repugnant to the employees, but it has such an inhibiting effect as to prevent the employees from performing their work with confidence and ease. Every employee has occasion to pause in the course of his work, to take a 'breather', to scratch his head, to yawn, or otherwise be himself without affecting his work. An employee, with reason, would hesitate at all times to so behave, if his every action is being recorded on TV.

Id.

In re FMC Corp., 46 Lab. Arb. (BNA) 335 (Mar. 23, 1966) (Mittenthal, Arb.), the employer installed a closed circuit television, with the employees' knowledge, in a plant to observe a receiving room from where the employer was losing property due to theft. That television received
tion of the United States labor force renders this a relatively ineffective overall method of regulation.

5. **Fair Credit Reporting Act and Similar State Statutes**

The statutes regulating credit reports are examples of device-specific statutes not providing a comprehensive solution to the workplace privacy issue. Viewed narrowly, they represent an important protection against a specific technique. Viewed broadly, they regulate one technique while, correspondingly, encouraging use of alternate techniques to accomplish the same end result.

The Fair Credit Reporting Act of 1970\textsuperscript{214} requires that employers obtain consumer credit reports on applicants and employees only for legitimate reasons,\textsuperscript{215} requires notice of adverse action taken as a result of such reports,\textsuperscript{216} and requires advance notice\textsuperscript{217} to the subject of the report in the case of certain investigative consumer reports.\textsuperscript{218} Some states have enacted statutes that are similar to the Fair Credit Reporting Act.\textsuperscript{219}

only a picture, not sound. *Id*. at 336 n.1. The arbitrator declined to address the union's argument that this violated human dignity and ruled strictly upon an interpretation of the collective bargaining agreement. *Id*. at 337 n.6. The arbitrator distinguished this situation from *Eico* because the collective bargaining agreement in this case had no "present conditions" clause. *Id*. In ruling favorably for the employer, the arbitrator found that the employees' privacy rights could not have been violated because the employees' actions simply were not private. *Id*. at 338.

Similarly, in *In re* Casting Eng'rs, 76 Lab. Arb. (BNA) 939 (May 20, 1981) (Petersen, Arb.), the employer installed a videotape camera system to monitor the punch-in clock on a continual basis. *Id*. Notice to employees was given in advance. The arbitrator ruled that the employer was justified in discharging certain employees under the "just cause" provision of the collective bargaining agreement, because when some of the employees punched in more than one card upon arrival, and other employees used those pre-punched cards upon their later arrival, their actions constituted theft of the employer's time. *Id*.


\textsuperscript{215} 15 U.S.C. § 1681b (specifically providing that a report may be obtained for "employment purposes"); see Peller v. Retail Credit Co., 359 F. Supp. 1235 (N.D. Ga. 1973) (holding that employer who terminated clerk after learning she had been arrested for shoplifting as child was not liable under Fair Credit Reporting Act), aff'd, 505 F.2d 733 (5th Cir. 1974).

\textsuperscript{216} 15 U.S.C. § 1681m(a) (such as denial of an employment offer based on information in the credit report).

\textsuperscript{217} *Id*. § 1681(d)(1).

\textsuperscript{218} *Id*. § 1681a(e).

\textsuperscript{219} See DECKER, *supra* note 36, at 79-80; 2 LEVESQUE, *supra* note 176, at II.1.8 to II.1.9; SMITH, *supra* note 176, at 10-11.
6. Polygraph Protection Act and Similar State Statutes

Perhaps the best examples of the long-term inadequacy of device-specific regulatory schemes are the federal and state statutes regulating use of polygraphs. The Employee Polygraph Protection Act of 1988 severely limits the use of polygraph examinations by private employers. As a practical matter, it has virtually eliminated the use of polygraphs in day-to-day employment decisions but has driven many employers to use alternative techniques to achieve the same goals.

In addition to the federal law limiting polygraph examinations discussed above, many states have statutes limiting the use of those exams by employers. In some cases, they are broader in scope and more strict than the federal statute. Some states have enacted legislation limiting the use of what are commonly referred to as paper and pencil honesty tests or integrity tests.

7. Unauthorized Opening of Mail

Another technique specifically addressed by federal law is mail opening. It is a federal crime to take a piece of mail from any mail carrier before it has been delivered to the person to whom it was directed if the person doing the taking has the intention to pry into the business or secrets of another. This would apply, for example, if an employer, wishing to know whether an employee were pursuing alternative employment opportunities, and with the required mens rea, opened mail delivered at the employer’s place of business.

220. 29 U.S.C. §§ 2001-2009 (1988). See generally Ching W. Chin, Note, Protecting Employees and Neglecting Technology Assessment: The Employee Polygraph Protection Act of 1988, 55 Brook. L. Rev. 1315 (1990) (providing an overview of employee protections in Polygraph Protection Act). Note also that the drug and genetic testing programs of private employers present issues similar to those raised by polygraph examinations. The Drug-Free Workplace Act of 1988 imposes affirmative duties on certain government contractors in this regard. 41 U.S.C. §§ 701-707 (1988). However, there is no comprehensive federal statute regulating drug testing in the private workplace in the manner the Employee Polygraph Protection Act regulates polygraph administration. Also, there is no comprehensive statutory regulation of genetics testing.


222. Id. at 72.

223. Decker, supra note 36, at 92-93 (listing statutes regulating polygraphs and truth-eliciting devices); Levesque, supra note 176, at II.1.8 to II.1.9; Smith, supra note 176, at 26-27; see also Moniodis v. Cook, 494 A.2d 212 (Md. Ct. Spec. App.), cert. denied, 500 A.2d 649 (Md. 1985) (holding that employee terminated for refusal to take polygraph has cause of action against employer under state statute).

224. See Decker, supra note 36, at 93 (discussing Maryland statute limiting use of inquiries into psychological matters); Arnold et al., supra note 14, at 65 (discussing legislation in Massachusetts and Rhode Island); see also Shepard, supra note 132, at 156 (listing states in which it may be argued that state law limiting polygraphs also extends to written honesty tests).


226. Id. ("design to obstruct the correspondence, or pry into the business or secrets of..."
but addressed personally to the employee.\footnote{Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1340 (9th Cir. 1987) (stating the general rule but finding employer not liable there because the letters in question had either not been mailed or had already been received by the employee, and because of doubts about existence of private cause of action).} Again, this is an example of an activity-specific prohibition that applies only in certain circumstances and that does not address the technological problems of today.

8. Privacy Acts and Similar State Statutes

Federal statutes, often considered to constitute comprehensive privacy legislation, are in fact quite limited in scope. Generally, it is intrusion by the government, not private parties, that is limited by these statutes.

The Privacy Act of 1974\footnote{5 U.S.C. § 552a (1988); see also Freedom of Information Act, 5 U.S.C. § 552 (compelling disclosure of certain information maintained by the federal government).} is an example. That statute provides a limited degree of privacy protection to private sector employees by limiting the disclosure of certain information maintained by federal agencies. For example, if information concerning an employee of a private employer were in the files of a federal agency because federal law required the employer to report that information, the Privacy Act would limit the ability of the federal agency to disclose that information to a new employer. Other federal statutes similarly limit the disclosure of private information in the hands of the federal government.\footnote{Access is limited to federally funded criminal justice information systems. 42 U.S.C. § 3735 (1988). Disclosure of school records is limited by 20 U.S.C. § 1232g (1988 & Supp. II 1990), and disclosure of tax records is limited by 26 U.S.C. § 6103 (1988 & Supp. II 1990).}

The Privacy Act also established a Privacy Protection Study Commission.\footnote{See generally Privacy Protection Study Commission, Personal Privacy in an Information Society (1977) The purpose of the commission was to examine individual privacy rights and recordkeeping practices in many environments.} That commission issued a report in 1977 that contained many recommendations applicable to employers in the private sector.\footnote{Id. at 37 (summarizing recommendations throughout report).}

Many states have enacted legislation similar to the Privacy Act. Those statutes are generally intended to limit the disclosure of information in state-government employee records.\footnote{Decker, supra note 36, at 78 n.393.} Many states, in a manner similar to the Right to Financial Privacy Act, limit the access of government agencies to bank records.\footnote{Smith, supra note 176, at 5-6.}

9. The Right to Financial Privacy Act and Similar State Statutes

The approach taken by federal and state statutes to financial privacy is similar to the approach taken by the Privacy Act. Generally government, not pri-
vate, intrusions are regulated. The Right to Financial Privacy Act of 1978 regulates the federal government in this respect.

These statutes are not a significant limitation on the efforts of employers to obtain information concerning the financial affairs of employees and prospective employees. The federal statute limits only the federal government in any attempt to review the "financial records" of customers maintained by financial institutions. The Act does not completely deny access of the federal government to those records; it simply limits the circumstances under which access is permissible and provides procedural protections for the customer when the federal government seeks access. For example, a request by a private employer to a bank to review the records of one of its employees would not be limited by the Right to Financial Privacy Act. Instead, the employee's primary protection against a disclosure of that type would be the employee's common law privacy rights and any rights under state banking statutes.

10. The Video Privacy Protection Act

The Video Privacy Protection Act of 1988, often referred to as the "Bork Bill," is an example of a statute implemented in reaction to a particular situation of concern.

---


235. "Government authority" is defined to include only agencies and departments of the federal government or an officer, employee, or agent of such department or agency. 12 U.S.C. § 3401(3).

236. Id. § 3401(2) (information pertaining to customer's relationship with financial institution).

237. Id. § 3401(5). Due to the definition of person in the statute, the term "customer" includes only individuals and partnerships of five or fewer individuals. Id. § 3401(4).

238. Id. § 3401(1).

239. A government authority is denied access to the financial records of a customer in a financial institution unless one of the specific exceptions in the Right to Financial Privacy Act applies. Id. § 3402. Correspondingly, a financial institution may not release those financial records to a government authority unless the provisions of the Right to Financial Privacy Act have been satisfied and the government authority has certified its compliance in writing. Id. § 3403. This limitation on the financial institution does not apply to notifying the federal government of information concerning possible violations of the law, or to protection of the bank's own interests, such as the filing of a proof of claim in a bankruptcy proceeding or the processing of a customer application for a government-sponsored program. Id. § 3403(c)-(d). For the exceptions to these general prohibitions on disclosure, see id. § 3404 (customer authorization); id. § 3405 (administrative subpoena or summons); id. § 3406 (search warrant); id. § 3407 (judicial subpoena); id. § 3408 (formal written request); and id. § 3413 (general exceptions).


misuse of information. The Video Privacy Protection Act limits the access of third parties to information privately maintained in an “electronic communication service” or a “remote computing service.”\textsuperscript{242} Similarly, it limits the access of third parties to “personally identifiable information”\textsuperscript{243} in the files of a “video tape service provider.”\textsuperscript{244} For example, it would prevent an employer from gaining access to the personal computer files of an employee maintained in a “remote computing service.”\textsuperscript{245} The act also prohibits a video rental store from disclosing its records of what titles were rented by a customer without the customer’s consent.\textsuperscript{246} Similar restrictions are imposed upon cable television companies, limiting their ability to disclose personally identifiable information about a customer, such as her viewing choices.\textsuperscript{247}

\section*{11. ERISA}

The Employee Retirement Income Security Act of 1974 ("ERISA")\textsuperscript{248} may provide remedies for employees subjected to artificial monitoring and surveillance in very limited circumstances. Specifically, section 510 of ERISA prohibits employers from discriminating against a participant in any employee benefit plan for exercising her rights under the plan and from depriving an employee of benefits under the plan.\textsuperscript{249} For example, it would likely be a violation of this protection if an employer used artificial monitoring to discover that an employee suffered from a serious medical condition, then discharged the employee in order to save the costs of funding benefits.\textsuperscript{250}

\section*{12. The Wiretap Act and Similar State Statutes}

The Electronic Communications Privacy Act ("Wiretap Act")\textsuperscript{251} demon-
strates the manner in which exceptions potentially devour a rule. This statute, at first glance, provides significant protection against some of the most common artificial monitoring and surveillance devices. However, as the following analysis shows, statutory exceptions make the protection virtually meaningless in the case of day-to-day monitoring and surveillance by employers in the private sector. An analysis of the Wiretap Act is also useful in that it provides an illustration of the problems of implementation.

The Wiretap Act makes it illegal to “intercept” willfully any “wire or oral or electronic communication.” Since this prohibition applies to private parties as well as the government, wiretapping by an employer to intercept an employee’s phone call made at work would be an illegal “interception” of a “wire communication” in some cases. Furthermore, recording by an employer of an employee's oral communications in the workplace would be an illegal “interception” of an “oral communication” in some cases.

There are criminal penalties for violation of the Wiretap Act. If the interception is illegal, the person whose communication is intercepted is additionally given the right to bring a civil action to remedy the unlawful intercep-
tion. For example, in *Awbrey v. Great Atlantic & Pacific Tea Co.*, there was evidence that the defendant employer installed wiretaps on business phones in stores where the plaintiff employees worked and during the times that they worked at those locations. The United States District Court for the Northern District of Georgia held that the employees could maintain a cause of action under the Wiretap Act even though they could not produce evidence of wiretapping of specific phone calls made by the individual plaintiffs.

Despite the relative ease with which the *Awbrey* plaintiffs were able to bring their action, the protection given to employees by these statutory prohibitions is quite limited for a number of reasons. First, the Wiretap Act is intended to apply only to content interception and not to transactional monitoring. Therefore, although there is uncertainty concerning the application of the Wiretap Act to certain forms of transactional monitoring, it does not reach the situation in which the employer activity is merely undertaken to determine whether a telephone call was made, as opposed to determining the substance of that call.

Second, the Wiretap Act contains a critical distinction between wire communications and oral communications. The definition of "oral communication" requires that it be "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." There is no such expectation-of-privacy requirement for a wire communication. The distinction between the two can be the difference between winning and losing a case. *Kemp v. Block* was a civil action in

---


259. *Id.* at 606.

260. *Id.* at 607.

261. See Shepard, supra note 132, at 232-33 n.57.

262. *Id.*

263. *Id.; see, e.g.*, Walker v. Darby, 911 F.2d. 1573 (11th Cir. 1990). In that case, a letter carrier brought an action against certain of his supervisors under section 2520 of the Wiretap Act alleging that unspecified activities had violated his rights under that statute. The United States District Court for the Northern District of Alabama granted summary judgment for the defendants on the grounds that the record was devoid of any evidence supporting the necessary elements of a state law privacy claim or a claim under the Wiretap Act. Walker v. Darby, 706 F. Supp. 1467 (N.D. Ala. 1989), rev'd, 911 F.2d 1573 (11th Cir. 1990). By contrast, the Eleventh Circuit Court of Appeals held that the plaintiff could raise a question of fact and thereby survive a motion for summary judgment without proving the contents of the specific conversations allegedly intercepted. *Darby*, 911 F.2d at 1578. Furthermore, the court of appeals emphasized that a plaintiff may have subjective and reasonable expectations of noninterception, even though he may not have a reasonable expectation of privacy in the workplace generally. *Id.* at 1578-79.

which the plaintiff alleged a violation of the Wiretap Act and an invasion of
the plaintiff’s privacy by a former co-worker. The plaintiff alleged that the
coworker had recorded the plaintiff’s argument with a shop foreman at
work. The place of the argument and the fact that it was conducted in loud
voices defeated the plaintiff’s claims on both theories because he had no rea-
sonable expectation of privacy.

Kemp may be contrasted to the result in United States v. McIntyre. The
defendants in McIntyre were convicted of violations of the Wiretap Act. The
defendants were the chief of police and a lieutenant in the police depart-
ment who suspected another police officer of leaking political information
damaging to the chief and of engaging in criminal activity. As a result, they
placed a microphone and a transmitter in a briefcase in the suspect’s office and
attempted to monitor his conversations. The court recognized that an estab-
ished regulatory scheme or a specific office practice may, at times, diminish a
reasonable expectation of privacy. However, a police officer does not give up
all protections by virtue of his chosen profession and does not have to expect
that random monitoring of oral communications would occur.

Third, the Wiretap Act contains two important exceptions to the intercep-
tion prohibition. One or both of these exceptions often will apply to employee
monitoring and surveillance. The first is the consent exception. Private per-
sons generally are not prohibited from intercepting a wire or oral commu-
nication when the person making the interception is a party to the communica-
tion or where one of the parties to the communication has given prior consent to
the interception. Accordingly, if the employee is speaking with a nonem-
ployee, the Wiretap Act will not prohibit the interception if there is express or
implied employee consent. Further, if one employee is speaking with another,

265. Id. at 1263-64.
266. Id. at 1263.
267. Id. at 1264-65.
268. 582 F.2d 1221 (9th Cir. 1978).
269. Id. at 1223.
270. Id.
271. Id.
272. Id. at 1224.
273. Id.
274. Id.
275. 18 U.S.C. § 2511(2)(d). See generally Glenn A. Gauravino, Annotation, Interception of
Telecommunication by or with Consent of Party as Exception, Under 18 USCS 2511(2)(c) and
(d), to Federal Proscription of Such Interceptions, 67 A.L.R. Fed. 429 (1984). This consent may
be given expressly by the employee. However, such consent is not to be interpreted as a “talisman
that automatically legitimates” all monitoring of an employee following the consent. Epps v. St.
Mary’s Hosp., Inc., 802 F.2d 412, 417 n.1 (11th Cir. 1986) (Kravitch, J., concurring in part and
dissenting in part); see also Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)
(stating that “[c]onsent under title III is not to be cavalierly implied”). Correspondingly, the
(holding that although police officer did not consent to the taping of personal call, officer should
have known he was on “monitored” line).
interception of the call is not prohibited if one of the two has consented. 278

The second exception is commonly known as the “business extension exemption” or the “ordinary course of business exception.” 277 The definition of “interception” in the Wiretap Act expressly excludes any telephone furnished to the user by a communications common carrier in the ordinary course of business and operated by that user in the ordinary course of business. 278

A series of federal cases construing this business extension exception created substantial uncertainties about its exact parameters. For example, in United States v. Harpe 279 the defendant was convicted of disclosing an unlawfully intercepted wire or oral communication under the Wiretap Act. 280 The defendant argued that the government had the burden to prove that the interception did not occur through the use of a telephone extension. 281 The Tenth Circuit agreed, but held that it is not just any telephone extension that falls under this rule, rather the extension used in the ordinary course of business. 282 The court stated, “We hold as a matter of law that a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business.” 283

United States v. Christman 284 was another prosecution for an alleged violation of the Wiretap Act. In that case, the regional security chief of a depart-

276. State laws concerning eavesdropping are frequently more stringent than the Wiretap Act. Decker, supra note 36, at 84-85; see also Furfaro & Josephson, supra note 1 (contrasting the one-party consent rule in New York to the stricter rule in Maryland). See generally Russell G. Donaldson, Annotation, Construction and Application of State Statutes Authorizing Civil Cause of Action by Person Whose Wire or Oral Communication Is Intercepted, Disclosed or Used in Violation of Statutes, 33 A.L.R.4TH 506 (1984); Eric H. Miller, Annotation, Permissible Surveillance, Under State Communications Interception Statute, by Person Other than State or Local Law Enforcement Officer or One Acting in Concert with Officer, 24 A.L.R.4TH 1208 (1983). For example, state laws often require the consent of both parties to a conversation before it may be recorded or intercepted. See Becker v. Computer Sciences Corp., 541 F. Supp. 694 (S.D. Tex. 1982); Morris & Bagby, supra note 2, at 176.


278. 18 U.S.C. § 2510(3)(a)(i). See generally Todd R. Smith, Annotation, Eavesdropping on Extension Telephone as Invasion of Privacy, 49 A.L.R.4TH 430 (1986); Janet B. Jones, Annotation, Application to Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USCS §§ 2510 et seq.), Pertaining to Interception of Wire Communications, 58 A.L.R. Fed. 594 (1982). There is also an exception under the Wiretap Act that exempts the operators of switchboards and communications common carriers when engaged in any activity incident to the rendition of service or the protection of the rights or property of the carrier as long as it does not amount to random monitoring. 18 U.S.C. § 2511(2)(a)(i). This exception is not considered in depth here because it is not of general applicability. However, it was the basis for dismissing a civil action by a former telephone company employee against the telephone company alleging that his private telephone calls had been monitored. Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392 (W.D. Okla. 1978), aff’d per curiam, 611 F.2d 342 (10th Cir. 1979).

279. 493 F.2d 346 (10th Cir. 1974).

280. Id. at 348.

281. Id. at 351.

282. Id.

283. Id.

ment store chain became concerned about a large number of improprieties, including solicitation of prostitution, theft, and improper telephone use, arising from a particular men’s shoe department.\textsuperscript{285} The store had a closed-dial telephone system to be used only for calls within the store or to other stores in the chain.\textsuperscript{286} It was possible to make calls outside that system but it was forbidden except in unusual circumstances.\textsuperscript{287} The defendant arranged for an extension phone to be installed in the department in question and proceeded to intercept and record conversations using that extension. The court found various grounds to allow the discharge of the defendant.\textsuperscript{288} First, the United States District Court for the Northern District of California emphasized that a phone system is designed to be a private system not within the scope of the Wiretap Act.\textsuperscript{289} Second, the court pointed out that oral communication must be made with a legitimate expectation of privacy in order to be protected by the Wiretap Act because “[i]t is doubtful that employees misusing a private telephone system are entitled to a reasonable expectation that the communication is not subject to interception as required by section 2520(2).”\textsuperscript{290} Third, the court held expressly that an extension telephone may not be an intercepting device under the Wiretap Act.\textsuperscript{291} Finally, the court held that random monitoring by communications common carriers is prohibited by the Wiretap Act but not by private system operators.\textsuperscript{292}

The business extension exception was considered again by the Tenth Circuit in \textit{James v. Newspaper Agency Corp.}\textsuperscript{293} In \textit{James}, a former employee sued her former employer alleging sex discrimination and violation of the Wiretap Act. The defendant employer had installed a telephone monitoring device on the telephones in certain of its departments. All of the employees were notified in advance and supervisory personnel then used the system to assist in training and instruction and to protect employees from abusive calls. The Tenth Circuit reconciled its holding here with its prior holding in \textit{Harpel}\textsuperscript{294} by ruling that the monitoring in this case was not surreptitious and was for a legitimate business purpose.\textsuperscript{295}

The First Circuit later had an opportunity to consider the business exception in \textit{Campiti v. Walonis}.\textsuperscript{296} In that case, the plaintiffs were inmates at a correc-
tional facility.\textsuperscript{297} The defendants monitored a call to which they were parties by the use of an extension telephone wired to the main switchboard.\textsuperscript{298} The First Circuit "flatly reject[ed]" the reasoning of the court in United States v. Christman.\textsuperscript{299} The court held that there is no general extension-telephone exception. The court found that the exception is based on the nature of the use of the extension and not on the nature of the equipment (i.e., an extension phone or not).\textsuperscript{300} Accordingly, the exception was not available to the defendants in Campiti.\textsuperscript{301}

Similar reasoning was then used by the Fifth Circuit in Briggs v. American Air Filter Co.\textsuperscript{302} to uphold the application of the business extension exception in another context. In that case, the branch manager of a business had particularized suspicions about the disclosure of confidential information by an employee to a competitor.\textsuperscript{303} Therefore, it was within the scope of the exception for the manager to listen in on an extension phone to the suspect employee's calls. First, the court rejected the reasoning of the Tenth Circuit in Harpel to the extent that it may be construed to mean that listening in surreptitiously on a phone conversation without the consent of either party may never be in the ordinary course of business.\textsuperscript{304} Second, the court found that the exception was available because the branch manager listened in only long enough to verify that business matters were the subject of the call.\textsuperscript{305} In its holding, the court declined to determine the exact point at which a violation would occur for listening in on personal matters or whether random monitoring can ever be justified under the exception.\textsuperscript{306} However, the court expressed skepticism that the interception of a nonbusiness call could ever be in the ordinary course of business, then pointed out that a limited interception of those calls might be appropriate if the employer was having difficulty controlling nonbusiness calls by employees.\textsuperscript{307}

The application of the Briggs reasoning is illustrated by Watkins v. L.M. Berry & Co.\textsuperscript{308} In Watkins, the plaintiff had been employed as a sales representative by the defendant. The plaintiff was aware of the defendant's policy of monitoring calls as part of its regular training program through the use of extension phones.\textsuperscript{309} The employees had been informed that personal calls

\textsuperscript{297} Id. at 389 (rejecting the holding in United States v. Christman, 375 F. Supp. 1354 (N.D. Cal. 1974)).
\textsuperscript{298} Id. at 390.
\textsuperscript{299} Id. at 392.
\textsuperscript{300} Id.
\textsuperscript{301} Id.
\textsuperscript{302} 630 F.2d 414 (5th Cir. 1980).
\textsuperscript{303} Id. at 420.
\textsuperscript{304} Id. at 419.
\textsuperscript{305} Id. at 420.
\textsuperscript{306} Id.
\textsuperscript{307} Id. at 420 n.8.
\textsuperscript{308} 704 F.2d 577, 581 (11th Cir. 1983).
\textsuperscript{309} Id. at 579.
were permissible and would be monitored only as long as necessary to determine their business or personal nature.\textsuperscript{310} The plaintiff received a call from a friend and discussed plaintiff's plans to consider another job. The plaintiff was fired the next day.\textsuperscript{311} The Eleventh Circuit held that the plaintiff had not consented to the interception of the particular call in question.\textsuperscript{312} The court stated first that Briggs does not stand for the proposition that a personal call may be in the ordinary course of business.\textsuperscript{313} Second, the court held that

\begin{quote}
a personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.\textsuperscript{314}
\end{quote}

The reasoning of Briggs was again applied in Abel v. Bonfanti.\textsuperscript{315} In Abel, a former employee alleged that his former employer had installed a voice activated recorder to continuously record all calls on one of four lines at a certain place of business. The court held that, despite the defendant's assertions that there was a business purpose for this activity and that it was done in a way so as to minimize the intrusion on personal calls, an issue of fact sufficient to defeat the defendant's motion for summary judgment existed.\textsuperscript{316}

Finally, the decision in Epps v. St. Mary's Hospital, Inc.,\textsuperscript{317} further confused the issues in this area. In that case, two employees of the defendant employer had a telephone conversation on a "ringdown line" connecting a dispatch office to a substation.\textsuperscript{318} Another employee overheard part of the conversation that dealt with a supervisor. That employee then went to the dispatch console and recorded the call.\textsuperscript{319} The court, in applying the rationale of Watkins and Briggs, stated:

\begin{quote}
[W]e hold that this was not a personal call. It occurred during office hours, between co-employees, over a specialized extension which connected the principal office to a substation, and concerned scurrilous remarks about supervisory employees in their capacities as supervisors. Certainly the potential contamination of a working environment is a matter in which the employer has a legal interest. Accordingly, we hold that this case falls within the "telephone extension exception."\textsuperscript{320}
\end{quote}

\begin{footnotes}
\item 310. Id.
\item 311. Id.
\item 312. Id. at 582.
\item 313. Id.
\item 314. Id. at 583 (citations omitted).
\item 316. Id. at 270.
\item 317. 802 F.2d 412 (11th Cir. 1986).
\item 318. Id. at 413.
\item 319. Id.
\item 320. Id. at 416-17 (footnotes omitted).
\end{footnotes}
In summary, these cases construing the business extension exception make it likely that unlimited monitoring by employers of employee calls on work phones is impermissible. The likely result is that employers may listen in on employee phone calls as is necessary for business purposes. Longer periods of listening to employees' personal calls are probably outside the exception. Yet the law in this area is far from certain. No standard for distinguishing personal from business calls has been established. Rather, such decisions are left to the discretion of the judge. The protections offered by the Wiretap Act are limited. The Act only applies to content interception. Furthermore, the exceptions to the prohibition on interception may indeed swallow the rule. Congress, in its proposals for legislation, must take into account the failings of device-specific prohibitions. In addition, any bill must have well-defined standards and exceptions to minimize interpretations by the courts that are detrimental to the privacy rights of employees.

13. State Personnel Records Statutes

Many states have laws that provide an employee access to his own personnel records upon request. For example, Connecticut statutes grant employees the right of access to their "personnel files" and the right to correct erroneous information in these files. The term "personnel file" excludes "medical records," "separately maintained security files," and certain test information. Therefore, an employee who is discharged as a result of information obtained by the employer through artificial monitoring and surveillance information might well have the right to see that information and correct it if erroneous.

Obviously, this right is severely limited as a practical matter. First, the employee may not even be aware that information of this type is in her file because of the very nature of the information-gathering process. No notice of the fact that the monitoring and surveillance will be or was carried out is required by the statute. Second, the information may be exempt from disclosure if it qualifies as a separately maintained security file. Despite these obvious limita-
tions, this area of the law potentially provides the greatest degree of protection to employees. But the lack of a significant number of appellate court decisions considering the rights of employees to challenge the records of an employer concerning the artificial monitoring and surveillance of employees would indicate that very few employees are yet pursuing this avenue.

In addition to these general personnel record protections, confidentiality of medical records is protected by many state statutes. Some states, such as Maryland, go further and limit the medical information that an employer may request from a job applicant or employee. In addition, employer inquiries concerning arrest records and personnel decisions based on arrest records without convictions are limited in many states. Similarly, many states limit access to information in the criminal justice information system, such as conviction records.

14. Drug Testing Statutes

Current federal statutes do not pervasively regulate the use of substance abuse tests in the private sector, although the Drug-Free Workplace Act of 1988 imposes drug-free workplace requirements upon certain federal contractors and grantees. By contrast, some states statutorily limit the use of urinalysis and blood tests by employers.

329. See generally Zitter, supra note 323 (discussing cases considering the validity, construction, and effect of statutes requiring employers to allow employees to inspect, review, and comment on personnel records).

330. Decker, supra note 36, at 88-89; Smith, supra note 176, at 14-17.

331. Decker, supra note 36, at 88 n.452.

332. Decker, supra note 36, at 89-90; 2 Levesque, supra note 176, at II.1.8 to II.1.9; Shepard, supra note 132, at 132-33; Smith, supra note 176, at 3-4.

333. Shepard, supra note 132, at 142-43; Smith, supra note 176, at 8-10.


15. Miscellaneous Statutory Limitations

Limited protections are available through a few state statutes that specifically target monitoring and surveillance activities. Connecticut has adopted a statute that, although providing significant protection, still is quite limited in scope. That statute prohibits employers from installing any electronic device or system in areas designed for personal health or comfort of employees or for the safeguarding of their possessions. West Virginia has adopted a statute regulating the use of telephone service observation. That statute makes it a misdemeanor to intercept a telephone conversation between an employee and a customer unless there has been advance notice to the employee and a phone not subject to such monitoring is provided to employees for personal use.

There are a multitude of other state laws that limit in some manner the ability of employers to collect or obtain other specific information about employees and prospective employees. Some states limit the use of fingerprints. Similarly, employers in some states are limited in their ability to test for sickle cell anemia. Some states have limitations upon the disclosure by cable television companies of information concerning their subscribers. Other states limit the disclosure of information by state agencies—for example, libraries, voting registration offices, and motor vehicle registration offices—of data bank information, such as the names of library subscribers. Taken as a whole, however, this patchwork quilt of state protection inadequately addresses the problems of employee monitoring and surveillance.

336. See, e.g., CAL. PENAL CODE § 653 (West 1988) (prohibiting two-way mirrors in washrooms and similar facilities); CONN. GEN. STAT. § 53-41a (1989) (prohibiting surveillance devices in department and clothing store dressing rooms available to the public); see also 2 LEVESQUE, supra note 176, at II.1.8 to II.1.9.; SMITH, supra note 176, at 71-93 (reflecting Texas' 1983 Electronic Surveillance Act). Some states regulate the use of "spotters." E.g., CAL. PUB. UTIL. CODE § 8251 (West 1965) (limiting use of spotters by public service corporations unless certain notice and hearing rights are provided to employees); NEV. REV. STAT. ANN. § 613.160 (Michie 1989) (prescribing that notice and hearing shall be afforded an employee prior to disciplinary action when such action is based on information gathered by a spotter); OHIO REV. CODE ANN. § 4999.17 (Baldwin 1991) (limiting the use of spotters by railroad companies).

337. CONN. GEN. STAT. § 31-48b (1987). The Massachusetts House of Representatives considered a broader prohibition of employer monitoring in 1969. In response to questions posed by the House, the Supreme Judicial Court of Massachusetts rendered an opinion that the statute likely violated both the United States and Massachusetts constitutions on the grounds of overbreadth. However, a concurring justice stated that it was likely that the legislature could adopt another statute that would "protect an employee's private and personal deportment and yet preserve the rights of the employer so as to pass constitutional muster." In re Opinion of Justices, 250 N.E.2d 448, 450 (Mass. 1969) (Spiegel, J., concurring). To date, no such legislation has been enacted. See also Dworkin, supra note 221, at 81-83 (noting other state legislative proposals).


339. DECKER, supra note 36, at 91 n.473; 2 LEVESQUE, supra note 176, at II.1.8 to II.1.9.

340. DECKER, supra note 36, at 95.

341. SMITH, supra note 176, at 5-6.

342. Id. at 14-16. Note the limits on bank records disclosure, id. at 5-6, the limits on disclosure of records in the criminal justice information system, id. at 8-10, the limits on disclosure of school records, id. at 21-23, and the limits on disclosure of tax records, id. at 23-24.
B. Common Law Remedies Available to Employees

In addition to these statutory remedies, an employee may assert that an employer's monitoring and surveillance is tortious. Although the protections given to employees by the tort law of privacy provide appropriate remedies in extreme cases, common law principles do not deal adequately with the practical issues raised by day-to-day legitimate uses of artificial monitoring and surveillance in the workplace. For example, any right of privacy is too easily bargained away. The essence of the tort is a reasonable expectation of privacy. If the employer simply makes it clear as a condition of employment that the employee has extremely limited expectations, then the employee has bargained away her right. In a situation of unequal bargaining power, this will certainly become the norm in the United States workplace.

1. Miscellaneous Tort and Contract Theories

The employment-at-will doctrine has been substantially eroded. As a result of this erosion and the enactment of various state and federal statutes, employees face a smorgasbord of theories of recovery if they are harmed by allegedly improper artificial monitoring and surveillance.

For example, an employee or applicant adversely affected by employer monitoring or surveillance might successfully bring an action for wrongful discharge if the particular activity were shown to violate public policy. Alternatively, that activity by the employer might be in violation of the terms of an express employment contract or might violate a contract implied-in-fact by, for example, a written personnel policy. Similarly, an employee might claim that an implied covenant of good faith and fair dealing in the employment relationship has been breached by the employer. If information about that

343. The Electronic Supervisor, supra note 6, at 89-90. As stated in that report, "[I]f there is no real basis in doctrines of privacy for objecting to the proverbial supervisor with a clipboard, there seems to be none to using a computer to do much the same thing." Id. at 90.

344. Rothfeder & Galen, supra note 9, at 75 (describing techniques commonly used by employers for this purpose, including waivers by employees, advance notification of surveillance to employees, and display of employer policies concerning surveillance). "For the most part, a company must be sloppy to get cornered." Id. For example, a recent article reports that a service, in exchange for a fee, will provide employers with an "all-purpose job application and waiver form" with which the prospective employee, among other things, purportedly waives all privacy rights. Kirsten A. Corbett, A Databank on Injured Employees, PRIVACY J., May 1990, at 4.

345. See Dworkin, supra note 221, at 59-60.

346. See generally Brossman, supra note 131 (providing an overview of the various theories of recovery available).


348. Id. at 331-33.

349. Id. at 333-37; see also Hineline v. Stroudsburg Elec. Supply Co., 559 A.2d 566 (Pa. 1989). In that case, the plaintiff alleged he had been wrongfully discharged after he disconnected the employer's surveillance system, a video system with audio capabilities. Id. at 567. The court refused to determine whether the system violated the Pennsylvania statute and upheld the dismissal of the plaintiff's complaint, which alleged wrongful discharge, intentional interference with contract, breach of covenant of good faith and fair dealing, punitive damages, and breach of
activity is conveyed to a third person in a manner that creates a false impression about the employee, there is potentially a defamation action against the employer. In some cases, employer activity might be so egregious as to rise to the level of outrageous conduct or the negligent or intentional infliction of emotional distress, or perhaps even false imprisonment. In most cases, however, the claim by the employee will be an invasion of privacy.

2. Privacy Invasion

There are four distinct types of privacy invasion. These are: (1) intrusion, (2) false light invasion of privacy, (3) appropriation, and (4) public disclosure of private facts.

In some cases involving the monitoring or surveillance of employees by their employers, "public disclosure" or "intrusion" provide a potential claim for relief. Generally, the public disclosure theory is available only when the employer transmits private information that arose out of its monitoring or surveillance activities to a third party.

Intrusion claims by employees are most common. The immediately following cases, based on the constitutional issues that arise when the government is the employer, demonstrate how employee expectations determine the reasonableness of the intrusion. Subsequently, the private employer cases demonstrate the limited scope of those expectations in the private workplace.

a. Government employees

The central issue in a case alleging that an employee's privacy rights have
been violated by an employer's monitoring or surveillance activities will be the plaintiff's expectations of privacy. Has there been an "intrusion" upon that expected privacy? The intrusion will generally be actionable only if the plaintiff in fact has a subjective expectation of privacy under those circumstances and if that expectation is reasonable as judged by societal norms.

Accordingly, criminal and civil cases involving searches of government workers at work are important. They are not, however, direct authority in support of a private employee's violation-of-privacy claim. The state action in a government worker's case raises the issue to a constitutional level. That state action is normally absent in the private worker's case. However, the same issue is central in both the case of the government and the private worker: Does the employee have a reasonable expectation of privacy while at work? The government worker cases, by analogy, establish both that workers may under certain circumstances have an expectation of privacy while at work and that such an expectation is easily bargained away by the employee.

United States v. Blok was a review of a government worker's conviction for petty larceny. Evidence of the crime had been seized through a warrantless search of the defendant's desk. The court found that the search in this case violated the defendant's constitutional right to privacy. However, the limited nature of that right is made clear by the following statement of the court:

We think appellee's exclusive right to use the desk assigned to her made the search of it unreasonable. No doubt a search of it without her consent would have been reasonable if made by some people in some circumstances. Her official superiors might reasonably have searched the desk for official property needed for official use. But as the Municipal Court of Appeals said, the search that was made was not "an inspection or search by her superiors. It was precisely the kind of search by policemen for evidence of a crime against which the constitutional prohibition was directed." In the absence of a valid regulation to the contrary appellee was entitled to, and did, keep private property of a personal sort in her desk. Her superiors could not reasonably search the desk for her purse, her personal letters, or anything else that did not belong to the government and had no connection with the work of the office.

The decision of the Supreme Court in Mancusi v. De Forte reinforces the conclusion that, although an employee may in certain limited circumstances have a reasonable expectation of privacy in the workplace, that right may easily be given away or diminished. In Mancusi, a union official was convicted of

356. 188 F.2d 1019 (D.C. Cir. 1951).
357. Id. at 1021.
crimes arising out of his misuse of union funds to organize juke-box owners and to compel them to pay "tribute." Evidence was seized through a warrantless search of an office that the defendant shared with other union officials. The defendant was present during the search and objected. The Court held that the union official had standing to object to the search and that it was unreasonable and in violation of his constitutional rights. However, the opinion suggests that the consent to the search could appropriately have been given not only by the defendant but by those with whom he shared the office, or by "higher-ups" in the union organization.

The possibility that a government worker's expectation of privacy at work may be given away is demonstrated by the case of United States v. Bunkers. In Bunkers, a postal worker's locker was searched in connection with an investigation of theft by that worker. The Ninth Circuit found that while the postal worker may have had a subjective expectation of privacy, she did not have a reasonable expectation of privacy. The union agreement in force specifically contemplated searches in the case of suspected criminal activity. The court stated:

Furthermore, we believe that Bunkers' voluntary entrance into postal service employment and her acceptance and use of the locker subject to the regulatory leave of inspection and search and the labor union's contractual right of search upon reasonable suspicion of criminal activity amount to an effective relinquishment of Bunkers' Fourth Amendment immunity in her work connected use of the locker.

The first case to extend to the civil context the concept of reasonable expectations of privacy of a government worker was O'Connor v. Ortega. A former chief of professional education at a state hospital brought an action against certain officials at the hospital. Those officials had become concerned about alleged improprieties in management by the plaintiff and about allegations of sexual harassment of female employees by the plaintiff. While the plaintiff was on administrative leave, the officials entered the plaintiff's office, searched it, and seized items from his desk and file cabinet. Ultimately, the seized items were used as evidence in an administrative proceeding that resulted in the plaintiff's discharge. The Supreme Court rejected the contention that a public employee may never have a reasonable expectation of pri-

359. Mancusi, 392 U.S. at 372.
360. Id. at 369.
361. 521 F.2d 1217 (9th Cir.), cert. denied, 423 U.S. 989 (1975); see also American Postal Workers Union v. United States Postal Serv., 871 F.2d 556 (6th Cir. 1989) (policy of employer, waiver signed by employees, and collective bargaining agreement negated reasonable expectation of privacy in lockers of employees).
363. Id.
364. Id. at 1221 (citations omitted).
366. Id. at 717.
vacy in his place of work. However, the Court pointed out that those expectations, in both the public and the private sector, may be reduced by office practices, procedures, and legitimate regulations. Nonetheless, in this particular case, the plaintiff had a reasonable expectation of privacy in at least his desk and file cabinets.

Despite this reasonable expectation of privacy, the Court in O'Connor declined to hold the search automatically unreasonable and in violation of the government worker's Fourth Amendment constitutional rights. The Court found neither a warrant requirement nor a probable cause standard to be appropriate, choosing instead to impose a standard of reasonableness. The reasonableness will depend upon a case-by-case balancing of the employee's legitimate expectations against the government's need for supervision, control, and efficient operation of the workplace. The case was remanded to make that determination.

b. Private employee searches

Employer searches of employees in cases of suspected theft have been a relatively frequent basis of privacy litigation. For example, an employee of K-Mart Corporation sued her employer for invasion of privacy in *K-Mart Corp. Store No. 7441 v. Trotti*. Employees of a local K-Mart store were provided with lockers at work but were not assigned a specific locker. They were also given a lock upon request, but the employer kept either the combination or a master key to the lock. Due to a shortage in locks, some employees were allowed to purchase their own locks. The plaintiff had done this, and the employer did not require her or the others purchasing their own locks to provide the employer with a key or the combination. Apparently, locker searches took place at the plaintiff's place of employment from time to time. However, this was not a policy that the employer had announced to its employees.

The complaint in *Trotti* arose out of the theft of a watch at the K-Mart store. The plaintiff was not suspected in the theft but a general locker search was conducted. After the search, the plaintiff found the lock on her locker hanging open and found the contents of her purse, which was in the locker at the time of the search, in considerable disorder. The plaintiff confronted her manager about this problem, and the fact of the search was initially denied.

---

367. *Id.*
368. *Id.*
369. *Id.* at 718-19.
370. *Id.* at 719.
371. *Id.* at 722.
372. *Id.* at 725.
373. *Id.* at 725-26.
374. *See supra* note 212 and accompanying text (discussing labor arbitration decisions in employee-search cases); *see also* Hall v. May Dep't Stores Co., 637 P.2d 126, 135-36 (Or. 1981) (holding that attempt by employer to force confession of theft out of employee was sufficiently outrageous to give employee cause of action against employer).
About one month later the search was admitted although there was conflicting testimony about whether the plaintiff's purse had been searched.876

The plaintiff was awarded $8000 in actual damages and $100,000 in punitive damages at trial.877 On appeal, the case was reversed and remanded because the trial judge had improperly instructed the jury.878 Specifically, the judge failed to specify that in order for an invasion of privacy to occur the intrusion must be "highly offensive" to a reasonable person.879 Despite ordering a new trial, the court held that the plaintiff had manifested, and the employer had recognized, a reasonable expectation that the contents of the plaintiff's locker would be free from intrusion and interference.880 The court, however, indicated that the result would have been different if the plaintiff had used a lock provided by her employer.

The appellate court also found that the jury instruction concerning damages had been improper.881 The instruction improperly conveyed the impression that the plaintiff could recover damages for mere embarrassment. Applicable state law required, however, actual mental anguish or physical suffering.882 The defendant also asserted that the award of punitive damages had been improper. The appellate court refused to find the award of punitive damages to be improper when the plaintiff's locker had been searched without any justifiable suspicion that she had stolen the watch.883

While the Trotti case exemplifies a willingness of courts to protect the privacy rights of employees, the holding is limited and cannot be applied to every invasion of privacy. The employee must have a reasonable expectation of privacy, and such expectations are easily bargained away.

c. Movies of worker activity

Taking movies of employees with a camera having audio capability may violate the Wiretap Act.885 Still photographs or videos of employees without sound will generally be analyzed under common law privacy principles.886 In Thomas v. General Electric Co.,887 for example, the employer had for thirty

376. Id. at 635.
377. Id. at 634.
378. Id. at 637.
379. Id.
380. Id.
381. Id.
382. Id. at 639.
383. Id.
384. Id. at 640.
385. See supra note 253 and accompanying text (stating that it is illegal to intercept any wire, oral, or electronic communication).

years engaged in the practice of taking motion pictures of its employees for the purpose of promoting safety and efficiency. The plaintiff, an employee, made a request to the defendant that his picture not be taken. The company nonetheless continued its practice of taking the motion pictures of its employees, including the plaintiff. The court characterized the case as a balancing of two conflicting rights—the managerial rights of the employer and the privacy rights of the employee. In carrying out this balancing process, the court held that this was not a violation of the plaintiff's right to privacy inasmuch as there was no showing that the plaintiff's health, welfare, or domestic situation was adversely affected or that the photographs had made him nervous or subjected him to undue or unfair criticism by fellow workers.

d. Monitoring of activities away from the workplace

Surveillance of employees away from their primary place of work may also give rise to a claim of a violation of the employee's right of privacy. For example, the plaintiff in McLain v. Boise Cascade Corp. injured his back while at work. In the course of a dispute concerning the termination of the plaintiff's workmen's compensation payments, Boise Cascade hired a private investigation firm to conduct surveillance of the plaintiff away from work to check on the validity of the plaintiff's injury claim. The private investigators took a number of photographs of the plaintiff. The activities filmed were those that a neighbor or passerby could have viewed, and the plaintiff testified that the contents of the film did not embarrass or upset him. Despite the fact that the investigators may have trespassed upon the plaintiff's property to take the films, the court found that the intrusion was not sufficient to give rise to a valid claim for violation of the plaintiff's right of privacy. The court recognized the interest of the defendant in determining the validity of the claim and held that the surveillance was not conducted in a manner that would be highly offensive to a reasonable person.

In International Union v. Garner subjects of the surveillance were union officials. In the course of attempts to unionize a plant in middle Tennessee, certain city officials conducted surveillance of the plaintiffs at or near union meetings. License plate numbers of persons attending the meetings were noted and traced, and the names of the attendees were transmitted to the plaintiff's employers. The plaintiffs then brought this invasion of privacy action against

388. Id. at 794.
389. Id. at 799.
391. 533 P.2d 343 (Or. 1975).
392. Id. at 347.
393. Id. at 346.
the city officials involved. The court held that there was no "false light" invasion of privacy because the information conveyed was not misleading.986 There was no public disclosure of private facts invasion of privacy because the matters disclosed were neither highly offensive to a reasonable person nor matters not of a legitimate concern to the public.987 There was no appropriation invasion of privacy for the obvious reason that there was no commercial use of the plaintiffs' names or appearances.987 Finally, there was no intrusion invasion of privacy because the actions of the plaintiffs were public in nature and did not create a reasonable expectation of privacy.988

Pemberton v. Bethlehem Steel Corp.999 once again involved the surveillance of a union official away from the workplace. In Pemberton, the plaintiff sued his employer because the surveillance was conducted under its direction. The plaintiff alleged claims of relief for intentional infliction of emotional distress, interference with the plaintiffs' marriage, conspiracy, and invasion of privacy. Bethlehem Steel had become aware of the plaintiff's criminal record and mailed information about that conviction to various union members. The company also placed the plaintiff under surveillance and mailed information about the plaintiff's marital infidelity to his spouse. Ultimately, this led to a divorce.

First, the court upheld a summary judgment for the defendant upon the claim for intentional infliction of emotional distress due to the absence of proof of actual emotional distress.400 Second, the court distinguished the separate legal grounds upon which the plaintiff based his invasion of privacy claim—intrusion and unwarranted publicity of the plaintiff's private life.401 The court found that transmitting the information to other union members and to the plaintiff's wife was not actionable because the plaintiff simply had failed to introduce any credible evidence establishing the involvement of the defendants in the circulation of the plaintiff's criminal history and details of the detective reports.402 However, the court found that the surveillance itself was significant enough to sustain a claim for relief based on the intrusion theory. The court indicated that surveillance conducted from public places would not be actionable. However, the surveillance went beyond that because listening devices were placed on motel room doors and surveillance was conducted from secret locations, such as stairwells.403

395. Id. at 189-90.
396. Id. at 190-91.
397. Id. at 190.
398. Id. at 191-92.
400. Pemberton, 502 A.2d at 1115.
401. Id.
402. Id. at 1116.
403. Id. at 1116-17.
e. Mail opening

The plaintiff in *Vernars v. Young* 404 was a twenty-seven-percent shareholder, an officer, and a director of a corporation. The defendant, a fifty-percent shareholder and the principal officer of that corporation, had allegedly opened and read the plaintiff's mail delivered to the corporation's office but addressed to the plaintiff and marked personal. The court held that these allegations, if proven, would constitute the tort of invasion of privacy on an intrusion theory.405

f. Questionnaires

In *Cort v. Bristol-Myers Co.*, 406 the plaintiffs, three sales representatives for the defendant employer, refused to answer certain confidential questions on a questionnaire sent to them by their employer. The grant by the trial judge of a motion for a directed verdict by the defendant on the plaintiffs' claims for invasion of privacy and bad faith termination of employment were upheld.407 The plaintiffs had refused to provide the type of information that they considered to be confidential or personal. Therefore, the court reasoned, there was at most an attempted invasion of privacy.408

g. Computer-based monitoring

Employee suits claiming a privacy invasion based upon ordinary (day-to-day) computer-based monitoring are also difficult to prove because of the courts' focus on the reasonableness of employees' expectations. The plaintiffs in *Barksdale v. IBM Corp.* 409 were hired on a short-term basis by an employment agency to participate in a study. The study concerned the legibility of various video display terminals to be used by bank tellers. The plaintiffs' claims based on fraud, intentional infliction of emotional distress, and violation of privacy were dismissed.410 The privacy claim was based upon intrusion. The court observed that "'[t]he Defendant's observation and recording of the number of errors the Plaintiffs made in the tasks they were instructed to perform can hardly be considered an intrusion upon the Plaintiffs' 'solitude or seclusion . . . or their private affairs and concerns.' " 411 Again, the fact that the intrusion took place in the course of employment swayed the court to decide in

---

404. 539 F.2d 966 (3d Cir. 1976).
405. Id. at 969.
407. Id. at 914.
408. Id. at 910.
410. Id. at 1383.
favor of the employer.

h. Wiretapping

In addition to potential violations of the Wiretap Act, it is possible that nonconsensual wiretapping of telephone conversations will constitute a tortious invasion of privacy.\(^{412}\) Several jurisdictions have recognized this potential in cases outside the employer-employee relationship.\(^{413}\) A claim of this type was raised against the former employer of the plaintiff in *Oliver v. Pacific Northwest Bell Telephone Co.*\(^{414}\) The plaintiff sought general and punitive damages on the basis that his former employer had secretly monitored his telephone calls, both during and immediately following the termination of his employment. The plaintiff had first become aware of that activity in the course of prior litigation between the same parties.\(^{415}\) In that prior litigation, the Supreme Court of Oregon rejected the argument that the employer was barred from enforcing the noncompetition agreement between the parties due to these alleged monitoring activities.\(^{416}\) The Supreme Court of Oregon, however, affirmed the trial court's dismissal of the employer's complaint on separate grounds.\(^{417}\) The Oregon Court of Appeals, in the later privacy invasion action, upheld the summary judgment ruling in favor of the defendant. The court recognized that other jurisdictions had found telephone conversation interceptions to be tortious under certain circumstances.\(^{418}\) However, in this case, the former employee had been unable to come forward with any evidence of the monitoring of his conversations in particular. The only evidence proffered was of monitoring activities of the defendant generally. The court relied on that absence of proof to reject both the tort claim and the claim under the Wiretap Act.\(^{419}\) The Oregon court rejected the reasoning of an Ohio court in *LeCrone v. Ohio Bell Telephone Co.*\(^{420}\)

In *LeCrone*, an Ohio court held that a prima facie case of invasion of privacy by wiretapping could be established where the means to intercept were

\(^{412}\) See generally Annotation, Eavesdropping as Violating Right of Privacy, 11 A.L.R.3d 1296 (1967).

\(^{413}\) See Fowler v. Southern Bell Tel. & Tel. Co., 343 F.2d 150, 156-57 (5th Cir. 1965) (applying Georgia law and holding that tapping of telephone without consent may be actionable intrusion upon privacy even without publication of surreptitiously obtained information); LeCrone v. Ohio Bell Tel. Co., 201 N.E.2d 533, 540-41 (Ohio Ct. App. 1963) (holding that telephone company and husband could be liable to wife for invasion of privacy after telephone company attached extension to wife's private telephone line during divorce proceeding). But see Schmukler v. Ohio-Bell Tel. Co., 116 N.E.2d 819, 826 (Ohio Ct. C.P. 1953) (finding no invasion of privacy for telephone company to monitor customer's calls to determine whether customer was violating a limited-use agreement).


\(^{415}\) Id. at 1297.

\(^{416}\) North Pacific Lumber Co. v. Oliver, 596 P.2d 931 (Or. 1979).

\(^{417}\) Id. at 943-44.

\(^{418}\) Id. at 946.

\(^{419}\) Id.

\(^{420}\) 201 N.E.2d 533 (Ohio Ct. App. 1963).
proven, those means were in existence for a substantial time, and a person with motive to intercept and physical access to those means was identified. At present, however, Ohio appears to be the only state providing such a liberal prima facie burden for privacy intrusion plaintiffs.

C. Summary

In summary, the current legal limitations do not adequately address the problems created by artificial monitoring and surveillance in the workplace. In addition to the limitations illustrated above, the statutory protections contain large gaps in coverage. For example, there is virtually no limit on collection of transactional information in the workplace. That transactional information can be used, for example, to construct personality profiles.

Further, the existing statutes simply fail to address issues unique to artificial monitoring and surveillance. For example, does the employee have a right to know the activity is taking place? Does the employee have access to the information collected so as to verify its accuracy?

There is, of course, the argument that normal market forces will naturally solve the problem. In other words, if it is true that workers become less loyal, more frequently ill, and less customer-sensitive in an environment in which artificial monitoring and surveillance devices are used, employers will naturally tend to limit or eliminate the use of these devices. However, the increased competitive pressures of a worldwide marketplace, the increased availability of the technology, and the increasing concerns of employers concerning substance abuse and employee theft make the use of the technology nearly irresistible. Recent news reports indicate that awareness of the problem is already taking place in some major United States businesses. In other situations, businesses are voluntarily adopting ethical codes to regulate internally the manner in which they deal with personal information. Although these market forces, and corresponding moves toward self-regulation, may well serve as a significant limiting factor, it is not safe to assume that these factors alone will provide an appropriate balance of employer and employee rights concerning this difficult issue.

421. See Gandy, supra note 7, at 62.
422. See The Electronic Supervisor, supra note 6, at 21. The report concluded that market forces will not curb the employer's use of monitoring because "many routine jobs are routine work that is subject to and indifferent to a high turnover rate. Thus it is not clear that 'natural' checks will be sufficient to ensure that monitoring is not abused." Id. But see Ronald Rosenberg, Most Workers in Survey Think Employers Use Electronic Means To Spy on Them, BOSTON GLOBE, Mar. 9, 1989, at 10 (reporting view of vice president and general counsel of Associated Industries of Massachusetts that electronic monitoring issues can be resolved without legislation).
423. See Bernstein, supra note 122, at 56 (reporting that many large U.S corporations are discovering that monitoring has adverse effects on service and therefore are beginning to reduce monitoring and emphasize quality); Markoff, supra note 50, at 7 (same).
424. Bernstein, supra note 122, at 56 (reporting the adoption of a "strict privacy code" by a major United States corporation to regulate its own use of personal information).
IV. Pending Legislative Proposals

Some experts are calling for a constitutional amendment to guarantee the right to privacy free from surveillance by private parties. However, it seems more likely that a legislative approach will be taken.

State legislatures over the past several years have periodically considered legislative proposals to regulate artificial monitoring and surveillance in the workplace. State proposals now under consideration take a variety of forms. Three bills are now pending in Congress that are intended to regulate "electronic monitoring" in the workplace. In the Senate, Senator Paul Simon introduced the Privacy for Workers and Consumers Act. In the House of Representatives, a substantially identical bill was introduced by Representative Pat Williams, and a similar bill was introduced by Representative Douglas Bereuter. These federal legislative proposals are receiving both strong support and strong opposition. A legislative fact sheet prepared by

425. Id.; Pamela Mendels, Making Room for the Bill of Rights Inside the Workplace: ACLU Expands Reach into Employee Rights, but Meets Opposition from Several Quarters, NEWSDAY, June 17, 1990, at 58 (indicating opposition to this approach, even within the ACLU itself).


428. See supra note 1 (discussing the Senate Bill).

429. See supra note 2 (discussing the House Bill and the Revised House Bill).


431. See Richard A. Barton, It's Time To Monitor the Bills, DIRECT MARKETING NEWS, Nov. 25, 1991, at 16 (noting that the senior vice president for government affairs of Direct Marketing Association opposes the proposals); Meg Fletcher, Bill Would Limit Surveillance of Comp. Claimants, BUS. INS., Sept. 23, 1991, at 3; Evelyn Gilbert, Insurers Battle To Eliminate WC
the Communication Workers of America describes, albeit in fairly hyperbolic terms, the problems that the proposed legislation seeks to remedy:

Secret monitoring is the merciless electronic whip that drives the fast pace of today's workplace in the service industry.

In essence, concealed surveillance combines the worst features of 19th century factory labor relations with 20th century technology, creating an electronic sweatshop.

In assembly-line environments, wage earners must produce at top speed under the unwinking eye of the computer taskmasters. These ever-vigilant machines "watch" every work activity that an employee performs, even counting the number of keystrokes per second he or she makes. The computer sets arbitrary work rules and then tracks the employee unceasingly to ensure that the standards are met. Standards are frequently ratcheted up, and evaluations become based on the minute details rather than on the final product or service.

The relentless assault of secret monitoring impels employees to care more about meeting a numerical standard measured by a lifeless computer than about meeting the service needs of a customer.183

The major elements of the proposed legislation433 now pending in the House and Senate are as follows.

(1) *Broad definition of "electronic monitoring":*

the collection, storage, analysis and reporting of information concerning an employee's activities by means of computer, electronic observation and supervision, remote telephone surveillance, telephone call accounting, or other form of visual, auditory, or computer-based surveillance conducted by any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photonic, or photo-optical system.184

---


434. House Bill, supra note 2, § 2(1). Because the pending proposals in the House and Senate, in their original form, are substantially the same, only the House Bill version is described here.

Presumably the drafters do not intend the House Bill to require that information be collected, stored, analyzed "and" reported before the activity constitutes "electronic monitoring." For example, video surveillance probably is intended to be covered if carried out, *even if* the tapes are destroyed (not "stored"), reviewed ("not analyzed"), or put into an employee's file ("not re-
(2) Broad definitions of “employer” and “employee.” The definition of employee includes former employees. Also, there is a separate definition of “prospective employee” designed to provide protection to employment applicants. The definition of employer includes all forms of entities, labor organizations, and federal and state governments. In addition, a minimum number of employees is not specified.

(3) Notice. If an employer engages in electronic monitoring, that employer must give all “affected” employees prior written notice of the form the monitoring will take, the “personal data” to be collected, the type of data that can be readily associated with a particular employee, the frequency of each form of monitoring, and the use of the personal data collected. The employer must also give notice of the interpretation of records that will be collected, the existing production standards and work performance expectation, and the methods for determining production standards and work performance expectations based on statistics generated through the monitoring process. In addition to this notice to currently affected employees, prospective employees must be informed “at any personal interview or meeting” of the potential electronic monitoring that may “directly affect” that person if hired, and the applicant must receive a copy of the notice given to currently affected employees upon
request.\footnote{440}

(4) Periodic warnings. A “beep” device or other notice that electronic monitoring is taking place must be given at periodic intervals unless the monitoring is continuous.\footnote{441} A separate requirement is included for “telephone service observation.” In that limited case, the customer must also receive notice that the monitoring is taking place.\footnote{442}

(5) Records access. If personal data is collected, an employee must have access to that data.\footnote{443} This does not apply to prospective employees or customers.

(6) Relevance. Any personal data collected must be relevant to work performance.\footnote{444}

(7) Disclosure limitations. Unless the employee consents in writing, any personal data collected by electronic monitoring may not be disclosed to third parties other than law enforcement authorities and the courts.\footnote{445}

\footnote{440}{House Bill, supra note 2, § 3(b). The Revised House Bill would require this notice at the “first personal interview” (as opposed to notice at “any personal interview or meeting”) and would require the notice to any employee who would be “affected” (as opposed to “directly” affected) if hired. Also, it would require that the general written notice be given not only upon request but whenever an offer of employment is extended. Revised House Bill, supra note 2, § 3(a)(4).}

\footnote{441}{House Bill, supra note 2, § 3(b)(3). The Revised House Bill would substantially alter this provision. First, the requirement of a “beep” or similar notice would apply only to monitoring that is “periodic or random.” Revised House Bill, supra note 2, § 3(a)(5). A separate notification provision would apply to “continuous” monitoring. \textit{Id.} § 3(a)(6). The notice in that event, i.e., the “beep” requirement, would apply only when the employer on a periodic or random basis “reviews data” (excluding data obtained via an “electronic card access system” or “data appearing simultaneously on multiple television screens”). Additionally, the right of an employer to later review data obtained by “continuous electronic monitoring” would be limited to data “relevant” to an employee’s work. \textit{Id.} § 3(a)(6)(B). Finally, the employer would be prohibited from using “beeps” and similar devices unless authorized by the statute. \textit{Id.} § 3(c).}

\footnote{442}{House Bill, supra note 2, § 3(b)(4). A bill was introduced in the House in July 1989 by Representative Ronald Dellums that would have required the consent of all parties to a telephone conversation before it could be intercepted. The bill also would have required all voice-activated tape recorders to include a “beep” warning and a warning label and would have prohibited the sale or advertising of those devices under certain circumstances. \textit{H.R. 2551, 101st Cong., 1st Sess.} (1989) (discussed supra note 2); see \textit{Dworkin, supra note 221, at 77-78} (concerning “beep” proposals in the states). \textit{See generally Nancy Blodgett, Employer Eavesdropping: Spurs Federal “Beep” Bill, 73 A.B.A. J. 24 (1987) (discussing “beep” proposal).}

\footnote{443}{House Bill, supra note 2, § 4. The Revised House Bill contains an exception to this general requirement of access by employees. Specifically, employees would not have a right of access until the completion of either the investigation or the disciplinary action, whichever were sooner. Revised House Bill, supra note 2, § 4(b).}

\footnote{444}{House Bill, supra note 2, § 5(a). The Revised House Bill would abandon the “relevant” standard, instead prohibiting intentional collection of personal data via electronic monitoring not “confined to the employee’s work.” Revised House Bill, supra note 2, § 5(a). It also would create an exception for the inadvertent collection of other data. \textit{Id.} In addition, it would specifically prohibit electronic monitoring in traditionally private areas, such as dressing rooms (except in limited situations). \textit{Id.} § 5(c).}

\footnote{445}{House Bill, supra note 2, § 5(b). The Revised House Bill contains an additional exception permitting public disclosure of information bearing on illegal conduct by a public official or on public health and safety. Revised House Bill, supra note 2, § 5(b)(2).}
(8) Limited use of results. In the case of performance evaluations and disciplinary action, personal data collected through electronic monitoring may not be the exclusive basis for the action, unless the employee is given the opportunity to review the data within a reasonable time after it is collected. Under no circumstance may any data obtained through electronic monitoring be the sole basis for setting production quotas or work performance expectations.

With limited exceptions, an employer is prohibited from collecting or disseminating any personal data obtained through electronic monitoring that describes the manner in which an employee exercises "rights guaranteed by the First Amendment" to the United States Constitution.

(9) Remedies. The secretary of labor is given the power to adopt administrative regulations and the right to bring injunctive proceedings and assess civil penalties. Private civil actions are also authorized in state or federal court within three years of the alleged violation. Furthermore, rights under the legislation cannot be waived except in settlement of a bona fide dispute.

446. House Bill, supra note 2, § 6(a). The Revised House Bill would additionally prohibit any action against an employee based on personal data obtained by electronic monitoring unless the required notice were given and the data collected were confined to the employee's work. Revised House Bill, supra note 2, § 6(a). Also, it contains antiretaliation provisions. Id. § 8.

447. House Bill, supra note 2, § 6(b). The House Bill referred to the "exclusive" basis for evaluations and disciplinary action, and the "sole" basis for production quotas. The Revised House Bill uses the "sole" basis in both cases. Revised House Bill, supra note 2, § 6(b).

448. House Bill, supra note 2, § 6(c). The Revised House Bill prohibits only "intentional" use in this manner and deletes the exceptions to the prohibition appearing in the House Bill. Revised House Bill, supra note 2, § 6(c).

449. House Bill, supra note 2, § 2(6).

450. Id. § 8.

451. Id. § 7(a)-(b). The Revised House Bill clarifies that the $10,000 maximum civil penalty is for each violation. Revised House Bill, supra note 2, § 7(a)(1).

452. House Bill, supra note 2, § 7(c). The prevailing parties would be entitled to recover reasonable costs, including attorney's fees. The Revised House Bill would clarify that the statute of limitations begins to run on the date the employee knows or reasonably could be expected to have known of the employer's violation. Revised House Bill, supra note 2, § 7(c)(3). Also, the Revised House Bill deletes language referring specifically to the right of an employee to bring an action on behalf of others similarly situated. Id. § 7(c)(2).

453. House Bill, supra note 2, § 7(d); see Kirsten A. Corbett, A Databank on Injured Employees, PRIVACY J., May 1990, at 4. That article reports that Employers Information Service ("EIS") will provide employers with a report on job applicants that includes a history of prior job injuries, a record of workers compensation claims, and a notation of whether former employers would rehire the subject of the report (without stating a reason for that conclusion). Id. EIS also provides employers with an application form that includes a waiver of all personal privacy rights, an agreement to submit to various types of tests, an agreement that the prospective employer may obtain various credit and background reports on the employee, and an agreement that employment, if extended, may be terminated without cause. Id. Note, however, that the Equal Employment Opportunity Commission has interpreted the Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12101-12213 (1988 & Supp. II 1990), to prohibit employer inquiries about worker's compensation history at the pre-offer stage. See 29 C.F.R. §§ 1630-1631 (1991).
V. LEGISLATIVE PROPOSALS

The time is now ripe for a solution to the problem of an inadequate legal structure protecting employees in the workplace. Due to the increased computerization of office work in the last fifteen years,\textsuperscript{454} the computerization of communications, and the rise of employee expectations concerning workplace rights, the problem must now be addressed legislatively.\textsuperscript{468}

First and foremost, this proposal for legislation must not be viewed as a complete solution to the issue of employee autonomy. It is simply one element of that overriding issue.\textsuperscript{466} For example, there is the possibility in the future of adopting a comprehensive "quality of work life" legislative package with coverage of artificial monitoring and surveillance of employees as just one of its many elements. This approach has already been taken in some foreign countries but does not appear to be a viable solution in the United States at this time.\textsuperscript{467} Nevertheless, Congress should not lose sight of the fact that it is time to begin studying such approaches carefully.

Furthermore, legislation at the federal level is the appropriate approach. The potential financial impact on a state due to lost business resulting from the enactment of such controversial legislation makes it unlikely that a comprehensive solution will be achieved in the states.\textsuperscript{468} Also, this is an area in which nationwide uniformity is critical to aid business compliance without undue hardship.\textsuperscript{469}

Additionally, it is critical not to view the question of the appropriate regulation of the artificial monitoring and surveillance of employees in a vacuum. If "device-specific" legislation is enacted, little will be accomplished. Employers will simply shy away from the regulated device and turn to other devices that may present even greater concerns. In some cases a particular device may be so dangerous that it warrants legislation which regulates that device specifically. For example, genetic screening in the workplace may well be appropriately regulated by a separate statute. However, the experience with polygraph examinations provides a lesson in this area. A comprehensive, device-specific statute was enacted at the federal level to cure the problems created by polygraphs. It has substantially curtailed polygraph use by most private employers, but it has driven employers to an arguably less reliable testing device, the "paper and pencil honesty test."\textsuperscript{460}

\begin{itemize}
  \item \textsuperscript{454} OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, PUB. NO. 287, AUTOMATION OF AMERICA'S OFFICES 8 (1985).
  \item \textsuperscript{455} See Note, supra note 18, at 1913-16 (arguing for a legislative solution). The author states that a "leap from current privacy doctrine to one protecting workers would involve considerable judicial activism." \textit{Id.} at 1914.
  \item \textsuperscript{456} See \textsc{The Electronic Supervisor}, supra note 6, at 23.
  \item \textsuperscript{457} \textit{Id.} at 22 app. A.
  \item \textsuperscript{458} See Furfaro & Josephson, supra note 1, at 3 (discussing the problems encountered by West Virginia in this area).
  \item \textsuperscript{459} See supra note 427 (listing some of the legislative proposals now pending in the states).
  \item \textsuperscript{460} Inwald, supra note 59, at 52.
\end{itemize}
It is, in fact, unlikely that even the most committed opponents of workplace monitoring and surveillance would argue that technology is the culprit.\textsuperscript{461} The solution obviously is not to prohibit the manufacture or sale of the technology except in the most unusual of cases. Rather, the solution is appropriate regulation of its use. Therefore, the legislation should focus on what might be labeled "due process in the private sector." Such due process would provide advance notice to employees of the monitoring, grant access to employee records concerning the monitoring, and create a procedural mechanism for employees to correct errors in the information collected. There are simply too many potential benefits for employers and employees to approach this issue from the standpoint of banning technology.

In arguing for a due process legislative approach, the counterargument will be made that any regulation is an undue interference with the basic employer-employee relationship. Of course the very essence of the employer-employee relationship is the employer's promise to compensate the employee in exchange for the employee's promise to perform services subject to the employer's control. This element of employer control necessarily implies that the employer will closely monitor the employee's activities on the job to ensure that the purpose of the agreement is being carried out. For example, it is common for an employer to monitor its hourly employees by requiring them to punch in and punch out on the time clock. Despite the fact that this type of monitoring may, at times, be annoying to the employees, most recognize it as necessary, and the argument cannot seriously be made that monitoring is inherently evil. Therefore, some employers may argue against legislation limiting the right to artificially conduct monitoring and surveillance, even if that legislation is narrowed to the modest scope proposed in this Article. Is there something unique about artificial monitoring and surveillance that should cause us to treat it in a manner different from other types of employee monitoring?

The answer is yes. The problem arises from the fact that the pace of technological development has simply outstripped the pace of change in employees' expectations about the type of monitoring to which they have agreed to subject themselves. Monitoring and surveillance techniques are potentially more intru-

\textsuperscript{461} See Marx, \textit{supra} note 53, at 12. As stated by one of the experts evaluating the policies of the hypothetical employer in that article, "Technology itself is not to blame for this state of affairs. In fact, information technologies, which represent a radical discontinuity in industrial history, could well lead to more reciprocity in the workplace, not less." \textit{Id.} (comments of Shoshana Zuboff). In her book, \textit{In the Age of the Smart Machine: The Future of Work and Power} (1988), Professor Zuboff makes the same argument.

She agrees that computers may end up being used mainly to routinize, subdivide and control jobs. But she argues that using them this way would be a mistake for the companies themselves: it would mean sacrificing the potential that computers offer for improving the products and services those computers help produce. To fulfill that potential, jobs will have to be redesigned to give employees the opportunity for more, not less, initiative—to allow them to interpret information the computer provides, and to make decisions based on that information.

sive today, even though they may be physically less intrusive in many respects. Today, the intensity of monitoring is extremely high, even continuous, and can more easily be hidden. Furthermore, it is difficult, if not impossible, for an employee who does not have access to the technology or records of its operation to refute the results. Finally, there is greater capacity to retain and retrieve records of the monitoring and surveillance through the use of computers.

As a result, the same employee who accepts the necessity to punch in and punch out might well be incensed to discover that her words and acts of the day have been recorded secretly on a hidden video monitor. Should the employee simply modify her expectations and learn to cope with these new monitoring techniques in much the same way that we have all learned to cope with other high-technology changes in our everyday life, such as radar guns in the hands of police officers monitoring traffic and hidden cameras monitoring the automatic teller machine?

Of course, the employee who is unwilling to modify her expectations always has the theoretical option to terminate the employment relationship or to assert pressure on the employer to cease the monitoring as a condition of maintaining the employment relationship. These theoretical alternatives are unlikely to be practical alternatives to the vast majority of workers, who do not have the luxury of quitting based on a difference in principle with the employer and who stand in an inferior bargaining position to the employer. Therefore, we must identify the point at which employer monitoring and surveillance crosses the line and becomes an unacceptable intrusion into private employee affairs that society is unwilling to tolerate.

The difficulty of this issue is well summarized in a recent article:

Most workplace privacy issues pose these kinds of difficult questions. They pit the needs of the company against the worker's feelings of dignity and worth. To sacrifice much of the latter would make work life untenable. So the United States must decide which rights of a citizen in society should extend to an employee in the corporation—and in what form. If employers don't voluntarily start this process, the courts or the legislatures will do it for them.

Once Congress decides that regulation is appropriate, it will be important in the regulatory scheme to differentiate among the various stages of the employment process. As stated in the Conference Board Report, "More than four-fifths of the survey participants in all three regions think that thorough solicitation of information from job applicants is the key to avoiding the need for more intrusive practices such as surveillance and monitoring." And according to one of the respondents to the survey described in the Conference Board Report, "You hire your own problems. Prevention remains the key. Monitoring and searching employees may deter theft, but such practices are unneces-

462. Gandy, supra note 7, at 62.
sary if proper attention is paid to the hiring process." Obviously, these comments overstate the case somewhat. Thorough hiring practices do not eliminate the need for careful supervision. But a regulatory climate that provides employers relatively greater flexibility at the front end might well make less flexibility at later stages seem more reasonable and palatable.

Specifically, much of the need for employers to rely upon various preemployment screening tests and posthiring monitoring and surveillance may arise from the employer's inability to obtain candid evaluations from prior employers. As reported in the Conference Board Report, the survey respondents were reluctant to give out salary history, performance appraisals, disciplinary and absentee reports, and psychological test scores about current employees to prospective employers. In fact, three-quarters of the survey respondents reported that they would not divulge information about current employees to prospective employers under any circumstances. A primary reason appears to be the threat of defamation or negligent referral litigation. Therefore, consideration should be given to legislation regulating the process of reporting on consumer credit history under the Fair Credit Reporting Act. This would provide employers disclosing information with a safe harbor in appropriate circumstances as well as provide employees with the right to challenge and correct inaccurate or outdated information.

Bearing these general principles in mind, a critical first element in any new federal legislation should be a definition of the regulated activity. Specifically, the statute should include a broad definition of the types of artificial monitoring and surveillance techniques covered in order to capture techniques now in use and to prevent circumvention by new technological developments. Although the definition of "electronic monitoring" in the Revised House Bill provides a good starting point for analysis, it needs to be improved in two respects.

First, the definition in the Revised House Bill would include many of the surveillance techniques currently employed in the American workplace, including systems for telephone call accounting and telephone service observation, video and still photos, sound recordings, interception of electronic mail and fax messages, computer-based monitoring, computerized time management, and biometric identification. Under the definition in the Revised House Bill, many information-gathering techniques used in the American workplace that should be excluded from the scope of this proposed legislation are in fact excluded. Nevertheless, the definition of electronic monitoring is both overbroad and underbroad. This results from two elements of the proposed definition: (1) the definition does not limit its scope to storage, analysis, and reporting of information originally collected by surveillance; (2) the definition refers only to "activities," not characteristics of the employee.

For example, assume that an employer requires employees to manually com-

464. BERENBEIM, supra note 6, at 5.
465. Id. at 8.
466. Revised House Bill, supra note 2; see supra note 2 (discussing the Revised House Bill).
plete an employee information form but enters the data into a computer for purposes of management analysis. This is, arguably, the "storage" and "analysis" of "information concerning an employee’s activities by means of computer." Similarly, assume that an employer uses a modem to obtain access to an employee-owned computer, located in the employee’s home, that contains personal data about the employee. If the information relates to the employee’s personal characteristics, as opposed to activities, it arguably would not be covered by the proposed legislation. Furthermore, the proposed legislation probably would not include any methods used to promote employee behavior, such as subliminal suggestion.

Second, the regulated activity should be labeled "artificial monitoring and surveillance" rather than "electronic monitoring." This more accurately describes the nature of the activity regulated and reduces the possibility that judicial interpretation will cause the statute to apply more narrowly than intended by its drafters. 467

467. This Article proposes the following definition of "artificial monitoring and surveillance."

SEC. 1 DEFINITIONS.

(1) Artificial monitoring and surveillance includes but is not limited to:

(a) The collection by an employer of "personal data" concerning an employee on the activities of that employee by "artificial means"; or
(b) The transmission by an employer of "artificial sensory messages" to an employee; or
(c) The storage, analysis, or reporting of personal data when that "personal data" was originally collected as provided in subparagraph (1)(a) above.

(2) An activity shall be considered to be "artificial monitoring and surveillance" even if the employer does not retain a record of the information collected. However, the following shall not constitute "artificial monitoring and surveillance" when conducted or obtained with the knowledge of the employee:

(a) Substance abuse testing;
(b) Integrity screening; commonly known as "pen and pencil honesty test";
(c) Genetic screening;
(d) Medical testing, including brain wave tests; and
(e) Skill testing.

(3) "Artificial monitoring and surveillance" shall not include the following: obtaining, maintaining, or analyzing any "consumer credit report" or "investigative report" subject to the Fair Credit Reporting Act or any polygraph examination subject to the Polygraph Protection Act.

(4) "Artificial means," as used in sec. 1(1)(a), refers to any method of collection of personal data concerning an employee by any method other than direct human observation. "Artificial means" includes, but is not limited to, any method by which information is received or transmitted, in whole or part, by wire, radio, electro-magnetics, photoelectric, or photo-optical system. "Artificial means" includes, but is not limited to, the following:

(a) Telephone call accounting;
(b) Telephone service observation;
(c) Computer-based monitoring;
(d) Review of electronic mail or computer files;
(e) Sound recordings;
(f) Video surveillance;
A new statute also should strengthen and clarify the Wiretap Act. Specifically, the Wiretap Act should be amended to require the consent of both parties to a telephone call before it may be intercepted. In addition, the Wiretap Act should be made expressly applicable to electronic mail, thus subjecting such activity to regulation by the new federal legislation and by the Wiretap Act.

The heart of a new statute should be a requirement of employee awareness that the monitoring and surveillance is taking place, unless there is particularized suspicion of the commission of a crime or similar circumstances. The advance notice requirement should be flexible and should apply to all persons who might be affected, including prospective employees, customers, and current employees. In other words, a specific written form of notice to employees by the employer should not be required nor should the statute focus on telephone monitoring as the only potential source of interference with customer rights. The statute should simply require advance notice to the persons affected in a manner reasonably calculated to apprise that person of the potential for artificial monitoring and surveillance of a particular type.

The notification provisions in the Revised House Bill, by contrast, are not sufficiently specific. For example, does a written notice posted on an employee bulletin board satisfy the requirement of "prior written notice?" Also, the notification provisions as proposed are unduly onerous in some respects. As presently drafted, the Revised House Bill would appear to require a new notice to all "affected employees" each time that one of the seven required elements of the notice is charged in any respect.

In addition to making employees aware that monitoring will take place, how it will be carried out, and what data might be collected that will be identified with the particular employee, the proposed notification to employees goes much further. It would require the employer to notify the employee concerning "existing production standards and work performance expectations." A notice concerning monitoring is not the appropriate method of informing employees

(g) Still photographs; and
(h) Computerized access or time control systems.

(5) "Artificial sensory message" means any message directed to the sense of sight, sound, taste, or touch of an employee which is transmitted in a manner not intended to appeal to the conscious thought process of that employee upon receipt by the employee. This includes, but is not limited to, the transmission of subliminal messages upon computer screens.

(6) "Personal data" means any information concerning an employee which may be readily associated with that particular employee for reasons including, but not limited to, the following:
(a) physical likeness or a photo or video image or sound recording;
(b) name;
(c) description;
(d) number; or
(e) identifying mark.

This subsection includes, but is not limited to, video tapes, still photographs, sound recordings, and computer printouts.
about those matters. More importantly, it tells employers who monitor electronically that they must disseminate this information to employees while it does not place a similar burden upon employers who choose not to monitor electronically.

The customer notification provisions of the pending legislation apply only to telephone call accounting. However, customers would understandably be concerned about other forms of monitoring, such as video surveillance, to which this notification provision does not apply.

The bills in Congress would limit the manner in which the data collected by electric monitoring could be used by the employer. That data could not, in most cases, be the "exclusive basis" for performance evaluation or discipline, nor could it be the "sole basis" for setting quotas. Once again, a substantial limit would be placed on employers who monitor electronically, while employers who choose not to do so would be unaffected. Further, the protection is empty in the sense that it could be avoided by having any other basis for the employer decision.

Any new federal statute should guarantee employees access to the records of the monitoring and surveillance. This approach is similar to that taken by many states with respect to personnel records generally. Particular procedures for access should be specified, and access should be limited to the employees affected and those other employees with a valid business reason for access to the records. Even so, access alone will not be enough. Specific procedures should be provided for challenging allegedly inaccurate or misleading data collected. In this arena, mandatory arbitration of disputes would be a useful tool to avoid unnecessary litigation while ensuring fairness of records maintained.

New legislation also should require maintaining confidentiality of the records of the monitoring and surveillance. Within the collecting organization, access should be limited to a discrete group with the need to know. Confidentiality procedures that will guarantee this in-house confidentiality should be mandated. Outside the collecting organization, disclosure should be made only in exceptional circumstances, such as employee consent or judicial process.

Finally, new legislation should provide administrative enforcement mechanisms, antiretaliation provisions, and civil remedies, including the right to recover costs and attorney fees. These remedies should not be subject to waiver before an alleged violation and should expressly be additional to any other remedies provided by law, including state legislation. The statute of limitations upon such a civil action should commence upon the date the employee knew, or reasonably should have known, about the alleged violation should be relatively short, perhaps one year.

Conclusions

Artificial monitoring and surveillance in the workplace should not be analyzed in narrow terms ignoring its broad potential. Nor should the likelihood of rapid, future technological change be ignored by using a device-specific approach destined in advance to become a legal dinosaur. Instead, this issue
should be approached as a key element of the overriding issue of the appropriate nature of the relationship between the employer and the employee in a society characterized by rapidly changing technology and values. In order to make certain that the many improvements in that relationship are not seriously diluted by technological innovations, federal legislation should now be adopted with the goal of maintaining the role of American workers as innovators and contributors at their places of work, not mere cogs in one of many complex machines. At present, the practical approach is to adopt legislation that does not cover all aspects of artificial monitoring and surveillance because some aspects of that activity, such as polygraphs, have been the subject of recent legislative activity. Instead, legislation should be enacted to fill the gaps in the existing legislative framework, and it should be viewed as merely the first step towards the long-term goal of enacting comprehensive worker-autonomy legislation.