NOTES

RESTRICTING ELECTRONIC MONITORING IN THE PRIVATE WORKPLACE

JULIE A. FLANAGAN

INTRODUCTION

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. . . . It was even conceivable that they watched everybody all the time. . . . You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and . . . every movement scrutinized.[1]

Although taken from George Orwell's futuristic novel, *1984*, this passage could easily have been written to describe the current workplace environment of approximately 20 million Americans.[2] Increasingly advanced technology allows employers to engage in a wide range of surreptitious surveillance activities, including monitoring all oral communications by employees, tracking every employee movement in the workplace, searching employee computer files, and reviewing employee electronic mail (e-mail) and voice

---

1. GEORGE ORWELL, 1984, at 4 (Harcourt Brace Jovanovich, Inc. 1977) (1949).

2. The computer magazine *MacWorld* recently hired an established computer consulting company to measure the use of electronic monitoring of employees. The company surveyed 301 businesses, representing a variety of industries and employing a total of almost one million workers. Charles Piller, *Bosses with X-Ray Eyes*, MACWORLD, July 1993, at 118, 120. More than 30% of the companies with 1000 or more employees responded that they routinely monitor employees. Among smaller companies, which generally lack the degree of computer sophistication of larger entities, 21.6% reported monitoring. *Id.* at 123. Extrapolating this data suggests that approximately 20 million Americans work in organizations that invade the electronic privacy of workers. These percentages reflect only monitoring performed through a computer and do not include any monitoring of employees by telephone. *Id.*

mail.[3] Like the Orwellian "Big Brother,"[4] employers can now monitor every aspect of an employee's workday.[5]

As a result of this rise in electronic monitoring[6] and the use of increasingly sophisticated software,[7] privacy in the workplace is growing as a labor and employment law issue. Businesses contend that monitoring to increase employee productivity, efficiency, and work quality is necessary in order to compete in the global marketplace.[8] Hence, employers maintain that monitoring in the workplace should remain an unrestricted prerogative of management. Labor organizations, on the other hand, argue that "concealed surveillance combines the worst features of 19th-century factory labor relations with 20th-century technology, creating an electronic sweatshop."[9] Just as unacceptable workplace conditions of the past, like twelve-hour workdays, necessitated government regulation, labor organizations have advocated restrictions to increase the quality of the workplace environment and to ensure a modicum of employee privacy and dignity.[10] In response, Congress has proposed legislation that would constitute the initial step in construct-

---

3. Of the employers who reported that they electronically monitor employees, 73.8% search employee computer files, 41.5% examine employee e-mail. 27.7% read network messages, and 15.4% review employee voice mail. *Id.* at 123.

4. A key distinction is that in Orwell's *1984*, the monitoring was performed by the government, whereas the monitoring this Note examines is instituted by the employer. Although monitoring by the government would be restricted by the Fourth Amendment of the U.S. Constitution, U.S. CONST. amend. IV, this restriction does not apply to private employer monitoring. *See infra* Section II(A).

5. For example, employers have monitored conversations in which employees revealed intimate details of a divorce or the existence of a medical condition. In one instance, an employee was instructed by her employer to seek medical attention because she was spending more than 12 minutes a day in the restroom. Julie G. Shoop, *Electronic Monitoring: Is Big Brother at the Office?*, TRIAL, Jan. 1992, at 13, 14–15; *see also infra* note 157 (detailing the manner in which many companies plan employee activity in increments of seconds).

6. Studies report that sales of software used to monitor employees are increasing by 50% per year. Laurie Flynn, *Big Brother Is Watching You Work: Programs Monitor Use of Computers*, HOUS. CHRON., June 20, 1993, at 4.

7. New types of software gaining popularity include programs capable of determining "what files were accessed, what programs were installed and whether anything was deleted . . . and even the length of the user's bathroom breaks." *Id.*

8. *See infra* Section I(B).

9. Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DEPAUL L. REV. 739, 808 (1992) (quoting COMMUNICATIONS WORKERS OF AM., LEGIS. FACT SHEET NO. 101–2–2, SECRET MONITORING 1–2 (1990)).

10. *See infra* Section I(C).

ing a legal framework in which to address workplace monitoring.[11] The pending Privacy for Consumers and Workers Act[12] (the Act) outlines the privacy rights of employees and the ability of employers to conduct monitoring.

After a brief overview of the sophistication of electronic monitoring and its current uses, Part I of this Note articulates the benefits of and objections to employer surveillance. Part II examines the current legal framework for private employer monitoring, including the federal and state remedies available to employees. Part III outlines the general provisions of the proposed federal legislation. It also discusses and evaluates the emerging legal environment and the resulting work atmosphere. This Note concludes that employer policies modeled under the Act's guidelines would create a work atmosphere advantageous to both employers and employees.

I. CURRENT USE OF ELECTRONIC MONITORING BY PRIVATE EMPLOYERS

A. *Forms of Monitoring*

Electronic monitoring makes it possible for employers to monitor the activities of their employees continuously and secretly. Although electronic monitoring includes a wide range of practices, three general categories dominate: computer-based monitoring; telephone call accounting and service observation; and video surveillance.[13]

Computer-based monitoring allows an employer to review specific activities of employees who work on computers. This practice is most pervasive in areas of employment that involve highly repetitive tasks.[14] For example, many mail sorters and data processors perform repetitive activities on computer monitors connected to a mainframe, allowing employers to record information such as speed.[15] Although computer-based monitoring is easiest when

---

11. On April 28, 1993, the Privacy for Consumers and Workers Act, H.R. 1900, 103d Cong., 1st Sess. (1993), was introduced by Representative Pat Williams of Montana. Senator Paul Simon of Illinois introduced a companion bill, the Privacy for Consumers and Workers Act, S. 984, 103d Cong., 1st Sess. (1993).

12. H.R. 1900, 103d Cong., 1st Sess. (1993).

13. *See* Kenneth A. Jenero & Lynne D. Mapes-Riordan, *Electronic Monitoring of Employees and the Elusive "Right to Privacy,"* 18 EMPLOYEE REL. L.J. 71, 72 (1992).

14. *Id.* at 73.

15. Piller, *supra* note 2, at 118. Although employee activity on a terminal not con-

repeated tasks are involved, professional and technical employees are not immune from computer-based monitoring.[16] If an employee's office is equipped with a full-featured computer network, a manager can eavesdrop on all components of an employee's computer work without the employee's consent and make all data transferred to the computer an "open book."[17] For example, supervisors can "view the contents of data files and electronic-mail messages, overwrite private passwords, and audit . . . time and activities on the network."[18]

Telephone call accounting is technology that records the length, time, and destination of phone calls.[19] Employers use telephone logs for various purposes, including limiting an employee's personal phone use.[20] Unlike telephone call accounting, service observation permits managers to monitor the substance of an employee's telephone conversations.[21] If telephone calls constitute an integral component of employees' work, such as for long-distance operators, airline reservation agents, and telemarketers, managers use service observation especially to review employees' conversations with customers.[22]

Almost all industries use video surveillance.[23] Employers videotape employees in a variety of situations to detect theft or violations of employer policies. Surveillance is usually a two-step process. Employers first install a camera that employees can see and then add a hidden camera.[24] Management also employs video

---

nected to the mainframe also can be monitored by the employer, the centralization provided by mainframe connection allows the employer more rapid access to the data, facilitating the monitoring of larger numbers of employees.

16. *Id.*

17. *Id.*

18. *Id.* at 118–19.

19. Boehmer, *supra* note 9, at 755.

20. *Id.*

21. Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1903 (1991).

22. *See* Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263, 1293 (1993). The Communications Workers of America (CWA), the major union representing telecommunications workers, estimates that employers monitor 400 million telephone communications between employees and consumers per year, an average of 750 calls per minute. Piller, *supra* note 2, at 118.

23. Jenero & Mapes-Riordan, *supra* note 13, at 73.

24. *See* Boehmer, *supra* note 9, at 757 n.84. The second camera may be greatly disguised, such as by hiding it in a sprinkling system or a heating duct. *Id.*

monitoring to record employee work habits such as movement on the assembly line.[25]

B. *Benefits of Workplace Monitoring*

Employers emphasize that monitoring is critical to improving employee productivity and to ensuring the quality of work.[26] For example, to increase productivity, employers can use electronic monitoring to plot the work rate of a particular individual and the work flow of a group of employees.[27] Additionally, computer-based monitoring can chart future work loads to increase productivity.[28] Monitoring also reduces the need for managers to give personal attention to employees because the computer can provide feedback.[29] A variety of industries use computer-based monitoring to train employees and to check the quality of their work. For example, service observation of telephone operators allows supervisors to oversee adherence to the employer's quality control guidelines on courtesy and salesmanship.[30] Employers also endorse monitoring as a basis for equitably evaluating an employee's overall performance, contending that monitoring functions as an unbiased measure of the quality of an employee's work.[31]

Moreover, managers use electronic monitoring to investigate possible employee wrongdoing or dishonesty.[32] For example,

---

25. Jenero & Mapes-Riordan, *supra* note 13, at 73. In addition to the listed categories, numerous monitoring variations exist. For example, public warehouses use radio signals to monitor forklift operators. Lisa Harrington, *Electronic Monitoring Bill: Labor's Latest Attack on Productivity*, TRANSP. & DISTRIBUTION, Sept. 1993, at 75 (quoting American Warehouse Association President Mike Jenkins). This electronic technology also permits the manager to measure an operator's efficiency. *Id.*

26. *Privacy for Consumers and Workers Act: Hearing on S. 984 Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor and Human Resources*, 103d Cong., 1st Sess. 27–32 (1993) [hereinafter *1993 Senate Privacy Hearing*] (statement of John Gerdelman, Senior Vice President, Customer Markets, MCI Communications Corp.).

27. Piller, *supra* note 2, at 120.

28. *Id.*

29. *Id.*

30. Robert J. Posch, Jr., *Can You Monitor Employee Phone Performance?* DIRECT MARKETING, Oct. 1993, at 100, 102 ("[R]andom monitoring is essential to ensure that employees adhere to [the employer's] strict quality-control guidelines pertaining to customer contact (courtesy, salesmanship, legal guidelines, etc.).").

31. *But see infra* note 62 and accompanying text (discussing employees' objections to the use of monitoring as a review tool).

32. One company uses "tiny, fish-eye lenses installed behind pinholes in walls and ceilings to watch employees suspected of crimes." Jeffrey Rothfeder et al., *Is Your Boss*

many managers view monitoring as a means to combat employee theft of goods and time. An estimated $370 billion is lost annually to employee theft in the United States.[33] Employers also are increasingly using electronic surveillance to protect trade secrets and other intangible property interests.[34]

As a separate justification, employers view surveillance as necessary protection against potential liability.[35] In addition to the traditional theory of respondeat superior, "employers now are frequently sued by persons injured by employees based on negligent hiring, retention, and referral theories."[36] The employer is potentially liable under these causes of action even if the employee was not acting within the scope of employment.[37] For example, when employees have access to sensitive data, employers risk liability if the employee either intentionally or negligently misuses the data and injures a third party.[38] Along with civil liability, employers may incur criminal liability for an employee's actions or omissions.[39]

Spying on You?, BUS. WK., Jan. 15, 1990, at 74. The U.S. Sentencing Commission encourages employers to use systems that are designed to identify and prevent criminal behavior in the workplace. *See* 18 U.S.C.A. app. 4 § 8A1.2 cmt. 3(k) (West Supp. 1994); 18 U.S.C.A. app. 4 § 8C2.5(f) (West Supp. 1994).

33. David W. Arnold et al., *Evaluating the Integrity Test*, SECURITY MGMT., Apr. 1990, at 62 (citing figures assessing employees' thefts of cash and merchandise at $200 billion in 1988 and employees' thefts of time at $170 billion in 1989).

34. *See, e.g.*, Boehmer, *supra* note 9, at 744; Piller, *supra* note 2, at 122.

35. However, a potential problem often overlooked by employers is the evidence that the electronic monitoring tapes may offer to potential claimants. *See, e.g.*, Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (involving employer tapes that were confiscated and used as the basis for an employee claim against employer).

36. Boehmer, *supra* note 9, at 746. Twenty-nine states allow a cause of action based on these theories.

> The essence of negligent hiring or retention liability stems from knowingly hiring (or retaining) an individual who is incompetent and/or possesses unreasonable risk to others. Hence, the primary way to avoid such liability is to conduct proper screening and investigation of prospective employees (or to discipline or discharge an employee who has been hired, but is clearly incompetent or poses a danger to others).

Id. at 746 n.28 (quoting Donald J. Petersen & Douglas Massengill, *The Negligent Hiring Doctrine—A Growing Dilemma for Employers*, 15 EMPLOYMENT REL. L.J. 419, 428–29 (1989–1990)).

37. *See id.* at 746.

38. *See, e.g.*, Djowharzadeh v. City Nat'l Bank & Trust Co., 646 P.2d 616, 618–20 (Okla. Ct. App. 1982) (holding bank liable when loan officer disclosed confidential loan application contents to a third party).

39. *See* United States v. Park, 421 U.S. 658 (1975) (finding that a company and its president could be criminally prosecuted under the Federal Food, Drug, and Cosmetic

Electronic monitoring also can improve compliance with company policies and safety guidelines.[40] For example, dashboard computers designed by trucking companies record a trucker's speed, the length of rest stops, and the idling time of the engine.[41] Trucking companies contend that this monitoring increases driving safety,[42] which in turn may reduce workers' compensation claims and insurance premiums.[43]

C. *Objections to Workplace Monitoring*

The primary objection to monitoring arises from its intrusion into an employee's privacy.[44] Even narrowly focused monitoring may intercept personal information.[45] Indeed, labor organizations have catalogued countless illustrations of invasions of employee privacy.[46] Some of the more egregious violations involve videotaping changing rooms. In one such instance, a Maryland hospital showed the tape of a nurses' locker room on an in-house cable channel.[47] More prevalent are instances of more subtle privacy violations. For example, an employee who was at home recovering from surgery received a phone call from a co-worker on break.[48] The employer monitored the conversation and "insisted that the convalescent return to the job, saying that if she was well enough to talk on the phone, she was well enough to come to work."[49] Labor organizations claim that such examples demonstrate that monitoring violates the privacy, autonomy, and dignity of both workers and those outside the workplace with whom they communicate.[50]

Act for allowing adulterated foods into commerce).

40. *See, e.g.*, Piller, *supra* note 2, at 121.

41. Rothfeder et al., *supra* note 32, at 74.

42. *Id.* However, labor leaders contend that companies unfairly use the dashboard computers to suspend or discharge employees: "If a trucker is just two minutes late, he can be brought up on charges." *Id.* at 75.

43. Boehmer, *supra* note 9, at 747.

44. The American Civil Liberties Union reports that it receives 50,000 employee monitoring complaints annually. *Washington Watch; Someone's Watching*, COMMUNICATIONSWEEK, July 12, 1993, at 29.

45. *See, e.g.*, David M. Katz, *Electronic Monitoring and The Odor of Fear*, NAT'L UNDERWRITER (PROP. & CASUALTY/RISK BENEFITS MGMT. ED.), Feb. 3, 1992, at 9.

46. *See, e.g.*, *1993 Senate Privacy Hearing*, *supra* note 26, at 18–19 (statement of Barbara J. Easterling, Secretary-Treasurer of CWA).

47. *The Electronic Whip*, ST. LOUIS POST-DISPATCH, June 28, 1993, at 2B.

48. *Id.*

49. *Id.*

50. *See* Boehmer, *supra* note 9, at 769–70. The privacy rights of the individual with

In addition to privacy concerns, employee advocates also cite the adverse health risks associated with monitoring as a reason to limit surveillance. A two-year study by the University of Wisconsin found that workplace monitoring causes physical and emotional health problems in employees.[51] The study found a higher incidence of headaches and other physical ailments, such as backaches and wrist pains, among monitored workers.[52] Moreover, monitored workers suffered greater fatigue.[53] Psychological problems included a 12% increase in depression and a 15% increase in extreme anxiety.[54] The results of the Wisconsin study mirror those of other studies,[55] including one by the National Institute for Occupational Safety and Health.[56] The Institute found that heavily monitored clerical workers "exhibited a greater degree of stress, depression, anxiety, instability, fatigue and anger."[57] Labor organizations emphasize that the ramifications of increased health

---

whom the employee is communicating often are overlooked. Companies that have assumed leading roles in consumer privacy concerns, including Citibank, American Express, and Equifax, "describe their electronic monitoring of employees as strictly limited." Piller, *supra* note 2, at 122–23. However, these companies would not release details of their privacy policies and "acknowledged surveillance practices beyond what would be allowed by some features of the congressional proposal." *Id.* at 123. For a discussion of this proposal, see *infra* Section III(A).

51. MICHAEL J. SMITH ET AL., UNIVERSITY OF WIS.-MADISON DEP'T OF INDUS. ENG'G, ELECTRONIC PERFORMANCE MONITORING AND JOB STRESS IN TELECOMMUNICATIONS JOBS 1 (1990). The CWA worked in conjunction with the University on the study. The study compared monitored workers at seven regional Bell Telephone locations with unmonitored workers at eight regional Bell locations. By using these two groups to control for other factors, the study attempted to establish a direct causal connection between stress caused from workplace monitoring and a greater incidence of physical and mental health infirmities. *Id.* at 3–4.

52. *Id.* at 5, 20.

53. *Id.* at 5–6, 21.

54. *Id.*

55. *See, e.g.*, Terry M. Dworkin, *Protecting Private Employees From Enhanced Monitoring: Legislative Approaches*, 28 AM. BUS. L.J. 59, 75 n.90 (1990). Dworkin cites a study at the University of California-Berkeley finding that workers in highly monitored jobs encountered more heart problems as a result of the stress than workers in non-monitored jobs. The researchers found that "[t]his was particularly true of women who had high demand-low control jobs," such as telephone operators. *Id.*; *see also* Peter A. Susser, *Electronic Monitoring in the Private Sector: How Closely Should Employers Supervise Their Workers?*, 13 EMPLOYEE REL. L.J. 575, 579–80 (1988) (reporting findings of the National Organization of Working Women that monitoring created employee stress and health-related problems).

56. *Electronic Monitoring Blamed for Increased Workplace Stress*, OCCUPATIONAL HEALTH & SAFETY LETTER (June 12, 1991).

57. *Id.*

risks extend beyond adverse effects to individual workers.[58] The greater rate of illness may affect the productivity of the entire workplace unit[59] and also can result in increased health costs to businesses.[60] The Office of Technology Assessment estimates that "stress-related symptoms cost United States industry $50 to $75 billion annually in absenteeism, medical expenses, and lost productivity."[61]

Although privacy concerns and health risks form the primary bases to attack monitoring, labor organizations discuss a variety of additional drawbacks. Employees frequently question the fairness of the company's use of monitoring to review employee performance,[62] despite management views of monitoring as a means to increase consistency in employee evaluations.[63] Employees also cite the potential negative effect on the overall workplace atmosphere.[64] Furthermore, surveillance may lower an individual's morale if, for example, an employee believes that monitoring indicates her employer's assumption that she is basically untrustworthy or unproductive.[65]

II. LEGAL ENVIRONMENT FOR PRIVATE EMPLOYERS

A. *Constitutional Constraints*

The Fourth Amendment to the U.S. Constitution protects individual privacy from government intrusion.[66] Hence, the protection of the Constitution extends only to public employees; pri-

58. *See, e.g., 1993 Senate Privacy Hearing, supra* note 26, at 19–20 (statement of Barbara J. Easterling, Secretary-Treasurer of CWA).

59. *See, e.g., id.*

60. *See, e.g.*, David D. Redell, *Safeguard Employees' Privacy*, SAN DIEGO UNION TRIB., Oct. 13, 1993, at B5.

61. Susser, *supra* note 55, at 579.

62. *See* Elizabeth Lee, *Technology, Privacy Clash on Job*, ORLANDO SENTINEL, Apr. 23, 1990, at C1, C3.

63. *See supra* text accompanying note 31.

64. *See, e.g.*, David D. Redell, *Stop Electronic Sweatshops*, CLEVELAND PLAIN DEALER, Oct. 4, 1993, at 7B ("When performance data is gathered without notification and used for mechanistic decisions about advancement, discipline or even firing, the work environment can become unbearable.").

65. *See* Boehmer, *supra* note 9, at 770. A union leader remarked that employers subscribe to the motto that "in God we trust. Others we monitor." *Id.*

66. *See* U.S. CONST. amend. IV (providing that "[t]he right of the people to be secure in their persons, houses, papers, and effects, *against unreasonable searches and seizures*, shall not be violated") (emphasis added).

vate employer behavior toward employees is not restricted.[67] Most states have a constitutional provision that reflects the proscriptions in the Fourth Amendment regarding search and seizure.[68] Some states, however, have specific constitutional guarantees of privacy that extend beyond the Federal Constitution's privacy rights.[69] Only California courts have held that the state constitutional right[70] of privacy applies with respect to both public and private employers.[71] In all other states, employees have successfully invoked the state constitutional right of privacy only after establishing that the government was the employer.[72]

In California, an employer may not violate an employee's reasonable expectation of privacy, as secured under the state constitution, unless the employer can establish a "compelling in-

67. *See, e.g.*, Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 397 (W.D. Okla. 1978) (dismissing portion of plaintiffs' complaint alleging that workplace monitoring of telephone conversation violated Fourth Amendment because private employer was not subject to the Fourth Amendment), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

68. *See* Jenero & Mapes-Riordan, *supra* note 13, at 80.

69. *See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein."); HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of property. . . . Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court."); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

70. CAL. CONST. art. 1, § 1.

71. Porten v. University of San Francisco, 134 Cal. Rptr. 839, 842 (Cal. Ct. App. 1976).

72. *See, e.g.*, Dworkin, *supra* note 55, at 60 n.5 (stating that only California extends protection to private employees); *see also* Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1130 (Alaska 1989) (finding that the right to privacy afforded by the Alaska Constitution does not extend to actions between two private parties).

terest."[73] This standard places a greater burden on employers than the "reasonableness" requirement mandated by the U.S. Supreme Court for Fourth Amendment challenges.[74] However, the employee still faces the difficult hurdle of demonstrating a reasonable expectation of privacy.[75] For activities such as the monitoring of changing rooms, for which the employee can establish the requisite expectation of privacy, the employer's heavier burden of providing a "compelling interest" may render some actions unconstitutional that would survive challenges under the U.S. Constitution. However, the change in the standard "is not likely to change the legal result in cases involving pure service observation and computerized work measurement."[76] Those claims will continue to fail because the employee cannot establish a reasonable expectation of privacy.[77]

---

73. *See* White v. Davis, 533 P.2d 222, 224–25 (Cal. 1975) (finding that the employer's failure to articulate a compelling interest could create a cause of action against the employer on state constitutional grounds of invasion of privacy); Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 84–85 (Cal. Ct. App. 1991) (finding that an employer must show a compelling interest to justify the invasion of privacy resulting from intrusive pre-employment questions); Luck v. Southern Pac. Trans. Co., 267 Cal. Rptr. 618, 632 (Cal. Ct. App.) (holding that a private employer operating a railroad did not demonstrate a compelling interest in testing a programmer for drug use), *cert. denied*, 498 U.S. 939 (1990).

74. Successful challenges based on the Fourth Amendment right to privacy typically must pass a two-prong test. First, the employee must establish a subjective expectation of privacy and demonstrate that the expectation was objectively reasonable. *See* O'Connor v. Ortega, 480 U.S. 709, 717–18 (1987) (O'Connor, White & Powell, JJ., & Rehnquist, C.J., plurality opinion). In evaluating a Fourth Amendment claim brought by a government doctor against the government for searching his office, the Court rejected the notion "that public employees can never have a reasonable expectation of privacy in their place of work." *Id.* at 717. However, the Court noted that "the expectation of privacy must be assessed in the context of the employment relation," including the "operational realities of the workplace" at issue. *Id.* For example, employers argue that an employee's expectation of privacy in computer communication is not objectively reasonable because employees are working during company time on a company computer with the password on file with the manager. *See* Piller, *supra* note 2, at 122.

Second, the employee must demonstrate that the interception cannot be justified by business reasons. *See Ortega*, 480 U.S. at 719–20 (stating that a government doctor's "legitimate expectations of privacy" must be balanced "against the government's need for supervision, control, and the efficient operation of the workplace").

75. *Luck*, 267 Cal. Rptr. at 626.

76. Jenero & Mapes-Riordan, *supra* note 13, at 80.

77. *See id.* at 79. State constitutional privacy claims involving workplace monitoring remain largely untested. In two recent disputes, employees have claimed that an employer's reading of e-mail messages violated the privacy provisions of the California Constitution. Alana Shoars, a former employee of Epson America, claimed that she was fired because she questioned her employer's practice of reading e-mail messages sent

B. *Tort Law Constraints*

Workers unable to ground a privacy claim in constitutional provisions may seek a common law tort action. Under the common law action for invasion of privacy, a private employee may claim that the electronic monitoring practiced by the employer constitutes an intrusion into the employee's privacy that would offend a reasonable person.[78] An employee alleging this tort must surpass several formidable obstacles. First, the employee faces difficulty in framing the work environment as a sufficiently private atmosphere.[79] Second, the employee must establish the monitoring conduct as highly objectionable.[80] Third, some courts maintain that publication of the information discerned from the surveillance must accompany the invasion of privacy.[81] The combination of these requirements typically defeats the employee's tort claim.[82]

---

among other employees. Shoars argued that the monitoring violated both the California constitutional right to privacy and the state eavesdropping statute. *See* Piller, *supra* note 2, at 122. An employer's interception of e-mail also was challenged on state constitutional grounds by two former employees of Nissan, who maintained that they were fired because they complained about managers reading personal e-mail messages in the company's system. *Id.*

78. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another, or his private concerns, is subject to liability to the other for his invasion of privacy, if the intrusion *would be highly offensive to the reasonable man.*" RESTATEMENT (SECOND) OF TORTS § 652B (1977) (emphasis added).

79. *See, e.g.*, Jackson v. Nationwide Credit, Inc., 426 S.E.2d 630, 632 (1992) (finding that the use of a speakerphone to monitor an employee's telephone call was not an unreasonable intrusion into private affairs, when monitoring was a routine and known practice of the employer).

80. *See* Billings v. Atkinson, 489 S.W.2d 858, 859 (Tex. 1973) (stating that eavesdropping forms the basis of a tort action only when the monitoring is conducted in a manner "to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities" (citation omitted)); Valencia v. Duval Corp., 645 P.2d 1262, 1264 (Ariz. Ct. App. 1982) (requiring that conduct be "extreme and outrageous" to constitute a claim for invasion of privacy); RESTATEMENT (SECOND) OF TORTS § 652B.

81. Although the *Restatement* identifies four possible categories of invasion of privacy, employee monitoring claims would fall only under the category "Intrusion Upon Seclusion" unless the employer engages in publication of the information obtained. RESTATEMENT (SECOND) OF TORTS §§ 652B–652E. Some courts do not view the four categories as distinct causes of action. Rather, they hold that the plaintiff must demonstrate both publication and intrusion into seclusion. *See, e.g.*, Barr v. Arco Chem. Corp., 529 F. Supp. 1277 (S.D. Tex. 1982).

82. An employee might claim that the employer's violation of privacy constitutes the tort of intentional infliction of emotional distress rather than invasion of privacy. However, for this cause of action, the employer's conduct must be extreme in degree, outrageous in character, and "atrocious, and utterly intolerable in a civilized community." Kaminski v. United Parcel Serv., 501 N.Y.S.2d 871, 873 (N.Y. App. Div. 1986) (citations

In *Thomas v. General Electric Co.*, an employee claimed that his employer violated his common law right to privacy by taking his picture despite his request "not to be photographed."[83] The pictures recorded the employee's movement in the workplace.[84] The employer stated that the pictures were taken in accordance with the employer's established policy of studying employee actions to facilitate increasing the efficiency of the operations.[85] The court dismissed the claim, finding that the plaintiff had failed to show that the monitoring exceeded the legitimate interest of the business.[86] *Barksdale v. International Business Machine Corp.*[87] also highlights the difficulty an employee faces when trying to prove a tort violation of invasion of privacy. The *Barksdale* plaintiffs alleged that IBM's monitoring of their work at computer terminals constituted an invasion of privacy. The court granted the defendant's motion for summary judgment, stating that "[t]he Defendant's observation and record of the number of errors the Plaintiffs made in tasks that they were instructed to perform can hardly be considered an intrusion upon the Plaintiffs' 'solitude or seclusion.' "[88]

The difficulty of maintaining a tort claim shows that the common law cause of action can "provide a source of protection for employees [only] in those extreme cases in which the employer's surveillance unduly infringes on personal conversations or activities without sufficient business justifications."[89] Typically, such situations involve employer monitoring in areas such as bathrooms and locker rooms. For instance, in *Doe v. B.P.S. Guard Services, Inc.*, the court held that a common law invasion of privacy occurred when videotape cameras surveilled models' dressing rooms.[90]

---

omitted).

83. 207 F. Supp. 792, 792 (W.D. Ky. 1962).

84. *Id.* at 793.

85. *Id.*

86. *Id.* at 799.

87. 620 F. Supp. 1380 (W.D.N.C. 1985), *aff'd*, 1 Indiv. Empl. Rts. Cas. (BNA) No. 2319 at 560 (4th Cir. July 16, 1986).

88. *Id.* at 1383.

89. Jenero & Mapes-Riordan, *supra* note 13, at 84.

90. 945 F.2d 1422, 1427 (8th Cir. 1991).

C. *Statutory Constraints*

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986,[91] was enacted in response to increasing privacy threats resulting from the growing use of sophisticated monitoring devices. Title III generally prohibits the monitoring of wire communications[92] and oral communications[93] unless one of the communicating parties has given consent.[94] However, the law provides two exceptions: for law enforcement agencies[95] and for employers.[96]

Law enforcement personnel may monitor lines if the surveillance is necessary in the investigation of certain criminal suspects.[97] The law enforcement agency must secure an order before commencing this monitoring.[98] Nationwide, courts authorize fewer than 1000 such taps annually.[99] Conversely, unlike the strictly channelled exception for law enforcement personnel, private employers have almost complete freedom to monitor employees.[100]

---

91. Pub. L. No. 90-351, 82 Stat. 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (1988)).

92. "Wire communication" is defined as any communication

> made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by a person engaged in operating such facilities for the transmission of interstate or foreign communications for communications affecting interstate or foreign commerce.

18 U.S.C. § 2510(1).

93. "[O]ral communication" covers "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation . . . ." *Id.* § 2510(2). The combined definitions of "wire" and "oral" communications clarify that the statute covers both wiretapping and electronic eavesdropping, such as bugging phones or listening on an extension. *Id.* § 2510(1)-(2).

94. Courts have construed the meaning of consent narrowly. For example, in Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983), the court rejected the notion of implied consent arising from knowledge that the conversation could be monitored.

95. 18 U.S.C. § 2511(2).

96. *Id.* § 2510(4)-(5).

97. *Id.* § 2516.

98. *Id.* §§ 2516, 2518.

99. Piller, *supra* note 2, at 118.

100. Supporters of new congressional action to limit workplace monitoring underscore the anomaly that private employers are the only group currently exempted from tight restrictions. As Senator Paul Simon stated, "[i]t is a sad irony that while the Federal Bureau of Investigation is required by law to obtain a court order to wiretap a conversation, even in cases of national security, employers are permitted to spy at will on their

Neither the manner nor the extent of employee surveillance is restricted. Moreover, employers are not required to provide any type of notice to employees. The only limitation that the law imposes on an employer monitoring wire communications of an employee is that the monitoring be "within the ordinary course of business."[101] In construing this requirement, courts have found a wide variety of monitoring to fall within the ordinary course of business.[102]

The courts have held an employer in violation of Title III only when the employer excessively monitored personal aspects of an employee's life. For example, in *Deal v. Spears*,[103] the U.S. Court of Appeals for the Eighth Circuit affirmed the district court's finding that an employer's electronic monitoring violated Title III.[104] In *Deal*, store owners believed that their employee had a role in a store burglary. The owners secretly recorded and listened to twenty-two hours of calls that contained highly personal information, including details of an extramarital affair.[105] Although the court found that some monitoring would have been justified,[106] it held that the extent to which the owners intercept-

employees and the public." *Privacy for Consumers and Workers Act: Hearing on S. 516 Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor and Human Resources*, 102d Cong., 1st Sess. 3 (1991) [hereinafter *1991 Senate Privacy Hearing*] (statement of Sen. Paul Simon).

101. 18 U.S.C. § 2510(5)(a). For a violation to occur, there must be an "interception" of the communication, which is defined as "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). Thus, there is no interception and no liability if the acquisition is through an instrument that falls outside the definition of "electronic, mechanical, or other device." The statute then exempts from the definition of acquisitions those occurring "in the ordinary course of . . . business." *Id.* § 2510(5)(a). For example, if a private person monitors another individual's telephone conversation, an "interception" has occurred under Title III, and the monitoring party may be held liable. However, if the monitoring party is a business, and the monitoring of the employee occurs within the ordinary course of business, there is no "interception" and therefore no liability.

102. *E.g.*, Epps v. St. Mary's Hosp. Inc., 802 F.2d 412, 416–17 (11th Cir. 1986) (monitoring phone call between employees by another employee acting beyond her authority deemed to be in the ordinary course of business); Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (holding that when an employer is concerned about the disclosure of confidential information, "it is within the ordinary course of business to listen in on an extension phone for at least so long as the call involves the type of information he fears is being disclosed"); Burnett v. State, 789 S.W.2d 376, 378–79 (Tex. Ct. App. 1990) (monitoring telephones to detect theft falls within ordinary course of business exemption).

103. 980 F.2d 1153 (8th Cir. 1992).

104. *Id.* at 1155.

105. *Id.* at 1155–56.

106. The court stated that the employers "might legitimately have monitored [the

ed personal phone calls was "well beyond the boundaries of the ordinary course of business."[107]

III. DEVELOPING LEGAL AND WORK ATMOSPHERES

A. *Proposed Legislation*

Because existing law generally fails to articulate employer boundaries or employee privacy rights, Representative Pat Williams of Montana reintroduced[108] the Privacy for Consumers and Workers Act (the Act) in 1993.[109] Under the Act, "electronic monitoring" includes all data collection by any technological device,[110] excluding only wiretapping and electronic transfer of payroll, insurance, or related information.[111] The Act would regulate any individual or business entity employing any number of workers.[112]

As currently proposed, the Act would require an employer to provide general notice to employees and prospective employees that the employer engages in workplace monitoring.[113] An employer could randomly monitor new employees without any advance notice of the specific surveillance during the first sixty days of employment.[114] For other employees, the employer would be

---

employee's] calls to the extent necessary to determine that the calls were personal and made or received in violation of store policy." *Id.* at 1158.

107. *Id.*; *see also* Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983) (holding that the monitoring of a personal phone call during the employee's lunch break was not in the ordinary course of business). If the employee is claiming a violation in an interception of an oral communication, rather than a wire communication, the employee must also demonstrate an expectation of privacy that the communication would not be intercepted. *See* 18 U.S.C. § 2510(2) (defining "oral communication" as including only that "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such an expectation").

State interception statutes largely mirror the federal laws and allow monitoring in the ordinary course of business. *See, e.g.*, Susser, *supra* note 55, at 589.

108. The employee privacy bills were initially introduced during the 1989–1990 term, but hearings were not held. Similar bills were introduced during the following congressional terms. Boehmer, *supra* note 9, at 739 nn.1–2. Although the House and the Senate have different versions of the bill, this Note discusses the House version.

109. H.R. 1900, 103d Cong., 1st Sess. (1993).

110. *Id.* § 2(1)(A).

111. *Id.* § 2(1)(C).

112. *Id.* § 2(3).

113. *Id.* § 4.

114. *Id.* § 5(b)(1).

required to provide individualized notice prior to actual surveillance.[115] This notice would have to state the days and hours when the monitoring would occur and the uses for the data collected.[116] Moreover, if the monitoring involved employee exchanges with customers, the customers would have to be notified of the monitoring either by a prerecorded message at the onset of a telephone call or by the prominent placement "in each of its customer bills [of] a statement that the employer is engaging in such practice."[117] In general, employers would be prohibited from randomly monitoring any long-term employee.[118] Notwithstanding these notice provisions, an employer could monitor any employee on the worksite without notice if the employer "has a reasonable suspicion" that the employee's action "violates criminal or civil law or constitutes willful gross misconduct."[119] Employers also could monitor employee activity if the basis of the investigation was possible employee abuse of workers' compensation.[120]

Electronic monitoring of bathrooms, locker rooms, and dressing rooms would be generally prohibited.[121] In addition, the Act would limit access to monitoring records[122] and would afford an employee the opportunity to review her records.[123] Moreover, an employer would not be able to evaluate work performance or set production goals or quotas solely on the basis of information acquired by monitoring employees.[124]

---

115. *Id.* § 4(b). Currently, only 31% of companies that monitor employees give advance warning. Piller, *supra* note 2, at 123.

116. H.R. 1900, 103d Cong., 1st Sess. § 4(b)(3)-(4) (1993).

117. *Id.* § 4(d).

118. *Id.* § 5(a). Employers could not randomly monitor anyone who has been employed for at least five years, but they could randomly monitor any employee who has been on the job for 60 days or less. They also could monitor employees who have been employed less than five years if those employees were in a work group of employees "engaged in substantially similar work at a common time." *Id.* § 5(b)(1)-(3).

119. *Id.* § 5(c)(1)(A).

120. *Id.* § 13(b).

121. *Id.* § 9(b). These areas could be monitored if the employer had a reasonable suspicion that monitoring would reveal violations of civil or criminal law. *Id.*

122. *Id.* § 9(d). However, an employer could disclose monitoring data to the public if the data contained evidence of illegal conduct by a public official or if the data would have a "direct and substantial effect" on public health or safety. *Id.*

123. *Id.* § 7(a).

124. *Id.* § 8(b)(1). Each violation of the Act would be punishable by a $10,000 civil fine. *Id.* § 12(a)(1). Moreover, employees could pursue private actions to seek equitable relief as well as attorney's fees and costs. *Id.* § 12(c).

B. *The Need for Congressional Action*

Employers possess great control over the functioning of the workplace.[125] Historically, however, an employer's ability to dictate the nature of the employment relationship has not been absolute. From early child labor laws enacted during the industrial revolution[126] to the Civil Rights Act of 1964[127] to evolving workplace safety standards,[128] congressional regulations have limited employer control in the workplace. Federal employment legislation is generally predicated on several findings. First, congressional action arises from employer behavior that abuses individual rights or notions of fundamental fairness or sparks public policy concerns.[129] Concerns of privacy, autonomy, and dignity implicated by current electronic monitoring abuses fall squarely within this ambit. Second, labor legislation arises when current regulation is found inadequate to protect these concerns.[130] Despite the rapidly growing use and sophistication of monitoring, the legal environment is largely structured on Title III, a statute enacted more than a quarter of a century ago.[131] Attempts to reformulate common law tort actions have failed, thus rendering the current legal limitations inadequate.[132] As the current proliferation of monitoring problems illustrates, normal market forces and

---

125. The continuing decline of organized labor has resulted in employers assuming even greater control over the workplace. Boehmer, *supra* note 9, at 741, 763.

126. *See, e.g.*, Barbara B. Woodhouse, *"Who Owns the Child":* Meyer *and* Pierce *and the Child as Property*, 33 WM. & MARY L. REV. 995, 1059–60 (1992).

127. Pub. L. No. 88–352, 78 Stat. 241 (codified in scattered sections of 42 U.S.C.).

128. *See, e.g.*, David J. Kolesar, *Cumulative Trauma Disorders: OSHA's General Duty Clause and the Need for an Ergonomics Standard*, 90 MICH. L. REV. 2079, 2082 (1992) (discussing prosecution of employers under the Occupational Safety and Health Act (OSHA) when they violate workplace safety standards by allowing employees to engage in harmful repetitive motions).

129. *See, e.g.*, Clyde W. Summers, *The Privatization of Personal Freedoms and Enrichment of Democracy: Some Lessons from Labor Law*, 1986 U. ILL. L. REV. 689, 723 (discussing Congress's responsibility to protect personal freedoms and noting "that it was in fact performing its function of protecting personal freedoms, as it did in the Wagner Act, Landrum-Griffin, Title VII, and OSHA").

130. *See, e.g., id.* ("Only through the institutions of government can we protect personal freedoms from private oppression. As lessons from labor law teach, that can be achieved only through congressional action . . . .").

131. *See supra* Section II(C).

132. With the current legal strictures, attempts to create a judicial solution require extensive reinterpretation of the law. In addition, purely judicial action would result in a piecemeal policy lacking national uniformity. *See* Note, *supra* note 21, at 1914–15.

self-regulation fail to provide an appropriate regulatory framework for balancing employer and employee rights.[133]

In a nation where large employers may have workers in multiple state and territorial jurisdictions, federal regulation of labor policies emphasizes the necessity of national uniformity.[134] A national labor policy such as the proposed Act would enable the formation of a uniform legal framework. Attempted action on the state level has been blocked by company threats to move business to a state without restrictions.[135] These abortive attempts by states to implement state statutes similar to the proposed Act underscore the need for nationally uniform treatment of employee monitoring.

As with other workplace issues arising from technological advancements, such as computer crime[136] and polygraph testing,[137] Congress should respond to the advances by enacting federal regulation. To replace the current amorphous legal standards, Congress should announce a national policy addressing an employer's ability to monitor employees and an employee's countervailing right to privacy in the workplace.

---

133. *See* Boehmer, *supra* note 9, at 806; Note, *supra* note 21, at 1898.

134. *See, e.g.*, Air Transp. Ass'n of Am. v. Professional Air Traffic Controllers Org., 667 F.2d 316, 323 (2d Cir. 1981) (recognizing need to "ensure a consistent body of federal labor law by preempting potentially inconsistent state court adjudication"); NLRB v. Committee of Interns & Residents, 566 F.2d 810, 816 (2d Cir. 1977) (holding that the need for uniform development of labor law mandates broad federal regulation), *cert. denied*, 435 U.S. 904 (1978).

135. For example, in 1981, West Virginia enacted a statute prohibiting telephone monitoring unless the employer adhered to strict guidelines, including using a warning tone audible to both parties to the conversation. However, the law was amended in 1986 to permit employers to monitor phone conversations provided that employees had access to unmonitored telephones for personal use and employees received a general warning that conversations could be monitored. W. VA. CODE § 61-3-24(c) (1981), *amended by* W. VA. CODE § 61-3-24(c) (1986). Labor unions claim that the driving force behind the amendment was AT&T's threat to cancel plans for a new office in the state capital unless the statute was altered. Susser, *supra* note 55, at 592.

136. *See* Note, *supra* note 21, at 1899-1902 (discussing this problem generally).

137. Employers use polygraph testing to check an employee's honesty, for example, when investigating an allegation of employee theft. For a general discussion on problems and concerns involving lie detector tests, see Dworkin, *supra* note 55, at 61-73.

C. *Assessing the Objections to the Privacy for Consumers and Workers Act*

The chief objection to a national policy constructing monitoring guidelines is that any restrictions on monitoring would reduce the productivity and quality of business.[138] One must, however, question the extent and even the presence of a conflict between productivity and privacy. Businesses maintain that a monitoring law would further inhibit attempts by the United States to increase worker efficiency and thereby place American companies at a disadvantage relative to international competitors.[139] Despite these claims, countries currently leading the global economy impose greater restrictions on employee surveillance than the proposed Act would.[140] For example, Japan and many European countries tightly restrict selective monitoring.[141]

The results of available case studies further question the supposed incompatibility of employee privacy rights and business productivity. In response to concerns that decreased monitoring would result in lower quality and productivity, the Office of Technology Assessment conducted a study of telephone operators and found that the elimination of secret monitoring resulted in "improved quality of service, fewer customer complaints, [a] decrease in absenteeism, [a] drop in management costs, [and a] reduction in employee grievances."[142] AT&T's Hotel Billing Information Systems in Tempe, Arizona, provides a particularly insightful case study. Unlike most AT&T system companies, the Tempe office does not monitor any employees.[143] Yet, the service level of the

---

138. *See, e.g.*, Jerry Jasinowski, *No Way to Fix the Problem*, CLEVELAND PLAIN DEALER, Oct. 4, 1993, at 7B ("Employers are concerned because this misguided bill [the Privacy for Consumers and Workers Act] would make it difficult to ensure the high productivity, quality products and top flight customer service that are so important in the competitive global economy of the 1990s.").

139. *See 1993 Senate Privacy Hearing*, *supra* note 26, at 30 (statement of John Gerdelman, Senior Vice President, Customer Markets, MCI Communications Corp.).

140. Piller, *supra* note 2, at 123. Additionally, American workers are more likely than Europeans to need protective legislation "because of the absence of strong employee associations, work environment laws, data protection commissions and legislations, and traditions requiring that work conditions be jointly set by labor and management." *1991 Senate Privacy Hearing*, *supra* note 100, at 47 (statement of Gary T. Marx, sociology professor at M.I.T.).

141. *1993 Senate Privacy Hearing*, *supra* note 26, at 2–3 (statement of Sen. Paul Simon).

142. *CWA Calls Monitoring "Menace,"* COMM. DAILY, June 24, 1993, at 3.

143. Marlene C. Piturro, *Employee Performance Monitoring . . . or Meddling*, MGMT.

operators was "rated equal to or better than any comparable office in the country by AT&T."[144]

Moreover, secretly monitoring employees is incompatible with evolving participatory schemes that American companies are currently implementing in an effort to regain leadership in international productivity.[145] Employee participation has been highly acclaimed for increasing productivity in the European Community and in Japan.[146] Likewise, cooperative labor-management relations, like the efforts at Ford,[147] are succeeding throughout the

---

REV., May 1989, at 32.

144. *Id.* Other companies that eliminated or reduced monitoring report similar results. After C&P Bell of West Virginia ceased the surreptitious electronic monitoring of employees, it received the top ranking of the entire Bell system in six of twelve customer satisfaction categories. Overall customer satisfaction was rated at 95.7%. *Id.*

145. Employee participation in American industry runs a spectrum of different degrees of involvement. At the minimal end, employee participation is limited to surveys and questionnaires. At the other end is intense employee involvement, such as profit sharing and employee ownership. Quality circles, semiautonomous work groups, and labor-management committees fall in the middle of the spectrum. Joseph B. Ryan, *The Encouragement of Labor Management Cooperation: Improving American Productivity Through Revision of the National Labor Relations Act*, 40 UCLA L. REV. 571, 579–80 (1992).

The quality circle is based on the concept that the individuals who are directly involved in production are in the best position to improve the quality of the product. Thomas C. Kohler, *Models of Worker Participation: The Uncertain Significance of Section 8(a)(2)*, 27 B.C. L. REV. 499, 506 (1986). A quality circle is defined as "a small group of workers who meet regularly on a voluntary basis to analyze problems and recommend solutions to management." HARRY KATZAN, JR., QUALITY CIRCLE MANAGEMENT 21 (1989). Motorola instituted quality circles and found numerous positive results, including a 25% increase in output and a decrease in turnover. Walter B. Scott, *Participative Management at Motorola—The Results*, *in* QUALITY CIRCLES 229, 232 (Roger W. Berger & David L. Shores eds., 1986).

One of the most stunning examples of the success of semiautonomous work groups is the GM-Toyota New United Motor Manufacturing (NUMMI) plant in Fremont, California. *See* Paul D. Staudohar, *Labor-Management Cooperation at NUMMI*, 42 LAB. L.J. 57 (1991). The productivity and quality problems intertwined with intense labor and management conflict led to the shutdown of the plant in 1982. *Id.* at 57. The institution of the participatory model resulted in a dramatic drop in grievances, less absenteeism, and an employee job satisfaction rate of 90%. *Id.* at 62. Moreover, the quality of the automobiles increased. *Id.* The company also has shown a profit, notwithstanding the promise not to lay off workers. *Id.* The success of labor-management committees, a more intense form of working groups, can be seen in a pilot program by AT&T. Ryan, *supra*, at 587.

146. *See* Robert E. Cole, *Learning from the Japanese: Prospect and Pitfalls*, *in* QUALITY CIRCLES, *supra* note 145, at 28, 28–41 (discussing the use of quality control circles in Japan).

147. The Ford program represents a cooperative effort between management and the United Auto Workers. It has resulted in increased productivity and product quality. The increased production arising from the quality circles at Ford was apparent in the redesign of assembly line mechanisms. The employees, through the quality circle discussions, added an automatic shutdown feature that improves quality and minimizes delay. Breakdowns

United States. Numerous business, labor, and government entities, including the Department of Labor, have stated that cooperative labor relations are "essential to the future success of the American industry."[148] Although employee participation programs vary widely, the basic idea is to improve productivity and efficiency by creating a more cooperative relationship between management and employees.[149] Thus, the adversarial relationship created by surreptitiously monitoring the workplace is directly antithetical to the underpinnings of participatory management programs.[150]

In addition to adversarial relationships, other factors associated with employee monitoring decrease productivity. Employers who monitor employees often experience high turnover rates as a result, which in turn decreases efficiency.[151] The decreased workplace morale[152] and increased health problems[153] caused by employee monitoring also affect productivity.[154] Furthermore, "[b]y making work into a numbers game, an employer often encourages counterproductive behavior."[155] For example, "[i]n order to meet

---

that previously cost $24,000 now cost $300. Ryan, *supra* note 145, at 582. Additionally, the number of grievances fell drastically after the program was implemented and employee job satisfaction greatly increased. *Id.* at 582–83. As one employee stated, "[t]he important thing is that [employee involvement] makes the worker on the floor feel like somebody." *Id.* at 583 (quoting Gerard Tavernier, *"Awakening a Sleeping Giant . . . ": Ford's Employee Involvement Program, in* QUALITY CIRCLES, *supra* note 145, at 222, 227).

148. BUREAU OF LABOR-MGMT. RELATIONS & COOPERATIVE PROGRAMS, U.S. DEP'T OF LABOR, FIRST INTERIM REPORT, U.S. LABOR LAW AND THE FUTURE OF LABOR-MANAGEMENT COOPERATION 25 (1987).

149. *See* Ryan, *supra* note 145, at 579–88.

150. Some analysts also find that monitoring creates an adversarial relationship among co-workers as well as between workers and management. *See* Marion Z. Goldberg, *Electronic Big Brother Spies on Workers,* TRIAL, Aug. 1990, at 75. This relationship is a product of the competition among workers that many monitoring programs instill. *Id.* An adversarial relationship among workers also contravenes the goals of participatory management.

151. *See* Jeff Kray & Pamela Robertson, *Enhanced Monitoring of White Collar Employees: Should Employers Be Required to Disclose?* 15 U. PUGET SOUND L. REV. 131, 164 (1991) (noting that turnover costs "include loss of the experience and training invested in current employees, the cost incurred while training replacement employees, and the potential loss of reputation in the market for future employees").

152. *See supra* notes 64–65 and accompanying text.

153. *See supra* notes 51–61 and accompanying text.

154. *See* Piller, *supra* note 2, at 122 (cautioning that "managers concerned with both productivity and containing health-insurance costs may find electronic monitoring to be self defeating" as studies link increased health problems to monitoring); *Snoops Put a Strain on Employee Loyalty,* BUS. WK., Jan. 1990, at 94 (noting relationship between employee morale and decreased productivity).

155. Redell, *supra* note 60, at B5.

unfair production goals, some workers feel forced to cut off customers, enter incomplete data, delete documents from other workers' files, or even drop paper clips into the machinery to slow it down."[156] Such counterproductive practices greatly decrease quality.[157]

Although the employer rationale for monitoring based on productivity and quality fails to withstand scrutiny, several employer justifications do remain, and the proposed Act, quite wisely, addresses these concerns. First, monitoring is an important tool to assist in proper training and to instill adherence to quality and safety guidelines. The Act allows monitoring to continue to serve these purposes by permitting random, unannounced surveillance of newly hired employees as well as monitoring of workers employed up to five years if the employee receives prior notice.[158] However, "training is an open process, designed for employee education—not an act of continuous, secretive spying."[159] Second, monitoring is an important way to ensure that employees work within the confines of company policy and the law. The Act embraces this function by allowing monitoring without prior notice when the employer has a reasonable basis to believe an employee has violated the law or grossly deviated from company practices.[160]

One business objection to the Act is its unnecessarily broad provisions. The definition of "electronic monitoring" arguably should be narrowed.[161] For example, the current definition would

---

156. Susser, *supra* note 55, at 580.

157. For example, the pressure to cut customer inquiries short regardless of the customer's needs is illustrated by the performance requirements for some airline reservation agents. At one airline agency, "agents are expected to average 109 seconds per call and 11 seconds between calls, during which time they catch up on paperwork. Workers . . . earn negative points for exceeding the expected average of 109 seconds per call and for taking any more than 12 minutes in breaks during each shift." Once a worker accumulated a set number of points, that worker could be fired. *Id.* at 581. This pressure to minimize "on the hook time" reduces the level of quality that consumers receive because employees focus solely on time efficiency. In one instance, a supervisor disconnected a call to an operator from a suicidal individual because "the length of the call was 'ruining' the average work time (AWT) of the operator. . . ." *1993 Senate Privacy Hearing, supra* note 26, at 20 (statement of Barbara J. Easterling, Secretary-Treasurer of CWA).

158. *See supra* Section III(A).

159. *See* Redell, *supra* note 60, at B5.

160. H.R. 1900, 103d Cong., 1st Sess. § 5(c) (1993).

161. In the proposed Act, electronic monitoring is defined as follows:

> [T]he collection, storage, analysis, or reporting of information concerning an employee's activities by means of a computer, electronic observation and super-

limit the monitoring of secure areas in airports and other areas where the employer should be able to monitor the area for safety continually regardless of the length of employee service. Similarly, the broad definition of "employee" should be restructured. Currently, the Act defines an employee as "any current, former, or leased employee of an employer."[162] Thus, if an employee quits, an employer would face potential liability for searching the former employee's computer files to retain important company information because that individual would still be a protected employee under the Act. Likewise, if a current employee were on leave, the employer might need to gain access to certain information, a situation for which the Act makes no provision. In these situations, the Act should allow an employer either to retrieve the necessary information or to request consent from the employee to retrieve critical data.

D. *Assessing the Merits of the Privacy for Consumers and Workers Act: The Emerging Work Environment*

Although employers maintain that unrestricted monitoring would further certain work objectives, expecting employees to forfeit all rights to privacy and autonomy on entering the workplace contrasts with the guiding principles of individual rights underlying American law.[163] The Act would vest employees with privacy, dignity, and autonomy rights in two ways. First, the Act would concretely grant employees certain enumerated rights, such as the right to notice and the right not to be monitored in a dressing area.[164] The Act also would provide a remedy for the violation

---

vision, telephone service observation, telephone call accounting, or other form of visual, auditory, or computer-based technology which is conducted by any method other than direct observation by another person, including the following methods: Transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature which are transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.

Id. § 2(1)(A).

162. *Id.* § 2(2).

163. *See* Jonathan J. Green, Note, *Electronic Monitoring in the Workplace: The Need for Standards*, 52 GEO. WASH. L. REV. 438 (1984) (outlining the importance of the right of privacy in American law); *see also* Note, *supra* note 21, at 1914 (discussing the privacy right as encompassing concerns for human dignity: "[i]f privacy actions were understood to encompass human dignity concerns . . . privacy doctrine would certainly provide modern workers with some protection from the current abusive practices").

164. *See supra* Section III(A).

of the listed provisions.[165] Second, the Act would create a sense of workplace empowerment among previously marginalized working groups, resulting from the return to the employee of a sense of control over personal information. Without the Act, employers can monitor freely almost every word and action of an employee. The employee lacks any control over personal information; the "ever-vigilant machines 'watch' every work activity."[166] By requiring prior notice and imposing restrictions on employer use of data collected, the Act would give employees some level of control. Employees would feel some minimal level of empowerment in the workplace relationship instead of feeling potentially victimized by the unfettered, unilateral control of the employer. Concomitant with the individual's sense of regaining control, the Act's limitations would alleviate the physical and psychological side effects of monitoring.

Yet, the Act recognizes that an employee's rights of privacy and autonomy are not absolute.[167] Although certain provisions might be excessively broad,[168] the guiding principles of the Act balance the right of the employer to maintain a business effectively[169] and the right of the employee to privacy.[170]

By improving employee working conditions through limited monitoring, the Act would especially affect the working environment in companies in which surveillance is heavily used. Implementing an articulate workplace electronic privacy policy[171] corresponding with the dictates of the Act would greatly reduce the adversarial relationship between employers and employees that is often a product of secretive monitoring, thereby fostering a more cooperative relationship. Such cooperative relationships would produce a "win-win" situation.[172] Employees would benefit from

165. *See supra* note 124.

166. Boehmer, *supra* note 9, at 808 (quoting COMMUNICATIONS WORKERS OF AM., LEGIS. FACT SHEET NO. 101-2-2, SECRET MONITORING 1-2 (1990)).

167. *See supra* Section III(A) (discussing the monitoring rights that employers retain under the proposed legislation).

168. *See supra* notes 161–62 and accompanying text.

169. *See supra* notes 158–60 and accompanying text.

170. *See supra* Section III(A) (discussing the monitoring prohibitions under the Act that vest the employee with certain privacy rights).

171. Passage of the Act would encourage employers to create an employment policy concerning electronic privacy. Currently, significantly fewer than half of employers surveyed—only 36%—have any written policy regarding employee privacy. Piller, *supra* note 2, at 123 (citing results of *MacWorld* poll).

172. *See supra* notes 145–48 and accompanying text (detailing the mutually advanta-

an improved working environment, and employers would profit from increased productivity.[173]

Realizing the opportunity to create this mutually advantageous situation, some companies already have entered into discussions with employees to create an internal electronic privacy policy closely resembling the Act. For example, Northern Telecom, with input from its employees' union, instituted a companywide policy that bans any secretive monitoring of employees. As the president of the CWA stated, "[I]n trials here in the U.S., when companies have suspended monitoring, their own measures of worker productivity and quality customer service have improved. The Northern Telecom policy prohibiting undisclosed monitoring puts the company on the cutting edge in ending a practice that fosters distrust, stress, and poor customer service."[174]

IV. CONCLUSION

Neither current laws nor market forces have produced an appropriate framework to control the proliferation of sophisticated monitoring by employers. As with other labor and employment issues that implicate questions about the intersection between employer practices and individual rights, congressional action should create the necessary legal framework. The enactment of the Consumers and Workers Privacy Act would achieve this goal by creating nationally uniform legal treatment of monitoring that would recognize both the legitimate managerial concerns of the employer and the privacy and autonomy rights of the employee.

Although management opposes the imposition of the Act, the long-term results of restrictions on monitoring would produce gains for employers as well as employees. Employers should view the creation of an electronic monitoring policy as one step toward forging the cooperative work atmosphere necessary for the United States to regain a competitive international edge.

---

geous ramifications when employees and employers engage in cooperative relationships).

173. *See id.*

174. *Northern Telecom Bans Secret Monitoring: CWA Agreement Sets Major Privacy Precedent*, PR NEWSWIRE, Jan. 30, 1992, *available in* LEXIS, News Library, Wires File. CWA also reached an agreement with US West, a telephone company in the Western United States. Shoop, *supra* note 5, at 14–15. Under the agreement, US West will provide employees with advance notice of monitoring. A spokesperson for US West stated that "[t]he philosophy behind [the change] was a natural evolution of a more open and trusting environment." *Id.* at 15 (second alteration in original).