PRIVACY OR DIGNITY?: ELECTRONIC MONITORING IN THE WORKPLACE

Lawrence E. Rothstein
PRIVACY OR DIGNITY?:
ELECTRONIC MONITORING
IN THE WORKPLACE

Lawrence E. Rothstein*

I. INTRODUCTION

The growth of electronic surveillance in the workplace has been phenomenal and has created a global problem. Such monitoring through video equipment, point of sale technologies, computer terminals, magnetic "active" badges, pen registers, telephone recording devices and numerical control machines now allows access to most, if not all, employee conversations and e-mail, and in many cases can record each movement or keystroke of an employee. While some of this recorded information is presently unused, employers are resorting to it more and more. In the United States, for example, a 1987 report by the Congressional Office of Technology Assessment estimated that six to eight million persons were subjected to such surveillance at work. A 1993 MacWorld study raised that estimate to 20 million workers. In 1996 the ACLU National Task Force on Civil Liberties in the Workplace estimated that 40 million workers were subject to

---

* Professor of Political Science and Associate of the Charles T. Schmidt, Jr. Labor Research Center, University of Rhode Island; attorney and member of Rhode Island, Massachusetts and Illinois bars. B.A. in Government, Carleton College, 1966; J.D. University of Illinois College of Law, 1969; Ph.D. in Political Science, University of Massachusetts, 1976. A version of this paper was delivered at the 11th World Congress of the International Industrial Relations Association, Bologna, Italy, September 25, 1998.


electronic surveillance. These estimates do not include the large number of employees subject to electronic monitoring of their telephone usage and conversations in such fields as telemarketing, financial and communication services. Including workers in these fields where monitoring is the norm, the American Management Association estimated that nearly two-thirds of medium to large businesses practiced one or more forms of electronic surveillance of their employees.

The concern in the two other countries considered in this Article, France and Italy, is manifest in their progressive efforts to limit surveillance and enhance workers' control, as will be discussed below. For example, the French national commission charged with registering nominative treatments of data recorded 34,426 cases in 1993, the highest number of new cases since 1982 and a 109% increase over 1990. Since that time annual registrations have grown each year. Since its inception in 1978 through December 31, 1997, the French commission has registered over 556,000 cases of businesses or government agencies collecting and electronically processing data identifiable to particular persons. Of these cases, approximately 45% relate to employees of the organizations doing the data collection.

This Article will undertake a comparison of the legal protection of workers from electronic surveillance and monitoring because there is markedly less protection in the United States than in the continental European countries. While the difference in strength of the U.S. and European labor movements might partially account for this, the example of France shows that even a continental European country with low union density provides significantly greater protection to workers than does the U.S. A Conference Board poll of its chief executive members along with

6. See discussion infra Part IV.
their Canadian and European counterparts has indicated that, while a majority of CEOs see electronic surveillance as ineffective and even detrimental to employee morale, the percentage holding these opinions is much higher in Canada and Europe than in the U.S.\textsuperscript{12} At least in part, the difference in legal protection stems from a differing conception of what values are being protected. In the U.S. the value of privacy is most frequently mentioned with regard to protection against surveillance;\textsuperscript{13} in continental Europe (and countries influenced by continental labor law), the value most frequently mentioned in the electronic surveillance context is human dignity.\textsuperscript{14} This Article shall argue that the legal protection of workers from electronic monitoring would be better served by deriving those protections from a concept of "human dignity" rather than of "privacy." It will proceed by first sketching the outline and origin of the two concepts and then by demonstrating their embodiment in legal texts regarding surveillance and monitoring in the workplace.

II. PRIVACY

The U.S. legal treatment of the concept of privacy is most akin to the philosophical perspective outlined by Ernest Van Den Haag. Van Den Haag's analysis exemplifies the possessive and territorial view of privacy. He notes that "[p]rivacy is best treated as a property right. Property grants an owner the exclusive right to dispose of what he owns. Privacy is the


\textsuperscript{13} For example, the classic Fourth Amendment "reasonable expectation of privacy" analysis used in cases of governmental wiretapping and surveillance. \textit{See e.g.}, Katz v. U.S., 389 U.S. 347 (1967), California v. Ciraolo, 476 U.S. 207 (1986); and the employment cases, \textit{see e.g.}, Briggs v. American Air Filter Co., 630 F.2d 414, 419 (5th Cir. 1980), Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983), Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 416–17 (11th Cir. 1986), that distinguish the monitoring of personal calls, deemed private, from business calls.

\textsuperscript{14} An example is the German Constitutional Court (BVerfG) and the Supreme Labor Court (BAG) have on several occasions confirmed that the German Constitution (Basic Law), Article 1, Section 1, (which states: "Human dignity is inviolable. To respect and protect it is the duty of all state authority") and Article 2, Section 1 (which states: "Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law") together establish protections for informational self-determination and autonomy of citizens and workers with respect to both government and private parties. \textit{See Judgment of July 16, 1969, 27 BVerfGE 1; Judgment of June 21, 1977, 45 BVerfGE 187, 229; Judgment of December 15, 1983, 65 BVerfGE 1; and Judgment of October 22, 1986, 53 BAGE 226, 233. See French and Italian examples in the text to follow.
exclusive right to dispose of access to one’s proper (private) domain.\(^\text{15}\) In an influential 1960 treatment, which still captures the legal treatment of privacy in U.S. law, William Prosser, former Dean of Boalt Hall Law School and noted commentator on U.S. tort law, placed the legal recognition of privacy tort claims into four categories. The one most relevant to our discussion of electronic surveillance and monitoring in the workplace was the “[i]ntrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.”\(^\text{16}\) The intrusion could be physical or electronic, but it had to be into an area which a reasonable person would find offensive or highly objectionable.\(^\text{17}\) Furthermore, the person intruded upon may lose, by consent or the existence of a special legal relationship, their right not to be so treated.\(^\text{18}\)

Privacy, in this sense, highlights a “possessive individualism.”\(^\text{19}\) Privacy implies notions of property, individualism, ownership and expectations with regard to the exclusion of outsiders without specific legal rights to the work premises.\(^\text{20}\) The protection of privacy connotes the possession by each individual of a zone of intimacy into which outsiders are not allowed to penetrate without the permission of the individual or without an extremely strong justification.\(^\text{21}\) Privacy is associated with one’s home, with intimate relations, and with premises under a person’s control.\(^\text{22}\) More fundamentally, this view of privacy stems from the individualist and property-oriented notion that an individual is the proprietor or possessor of her or his own person and capacities, for which nothing is owed to society.\(^\text{23}\) Privacy is territorial and is seen as a possessive right that may be alienated preemptively and wholesale.\(^\text{24}\) This possessive, territorial view of privacy finds clear expression in the workplace.

When a worker sells her capacity to labor, she alienates certain aspects of the person and puts them under the control of the employer. Thus in the U.S., workers in the workplace, except occasionally in restrooms and

17. See id. at 389–91.
18. Id. at 391.
20. See id.
21. See id. at 263.
22. See id. at 142, 264.
23. See id. at 3, 263.
employee locker rooms, are not generally protected from surveillance on the grounds that the premises and equipment are possessions of the employer and the employee can have no legitimate expectation of intimacy or of protection from employer intrusion. The employee, in the employment-at-will setting, has implicitly consented to the employer’s right to monitor the employee closely “for any reason, no reason, or even reason morally wrong” or lose her job.

III. HUMAN DIGNITY

Where Anglo-American jurisdictions emphasize the concept of privacy in their legal protection of workers from monitoring and surveillance, continental European countries manifest a concept of human dignity more related to notions of community and citizenship than property. French, Italian, German and Spanish do not even have a direct equivalent of the English word ‘privacy.’ The concept of human dignity is a social one that promotes a humane and civilized life. The protection of human dignity allows a broader scope of action against treating people in intrusive ways. While also concerned with intrusions upon a person’s intimacy and autonomy with regard to her or his private life, human dignity, unlike privacy (at least as embodied in U.S. law), is primarily concerned with actions that reduce a person’s status as a thinking being, a citizen and a member of a community. As Alan Westin stated in his earlier work linking autonomy and dignity to advocate attention for privacy protection: autonomy is grounded in a “fundamental belief in the uniqueness of the individual, in his basic dignity and worth as a creature of God and a human being . . .” and results in “the desire to avoid being manipulated or dominated wholly by others.” At work, human dignity is denied by treating the employee as a mere factor of production with fixed capacities and vulnerabilities determining her behavior and ignoring both the worker’s individuality in the


face of statistical probabilities and the human potential to overcome or compensate for physical obstacles.  

The worker's dignity is denied when she is treated as a mechanism transparent to the view of others at a distance and therefore manipulable or disposable without the ability to confront the observer.

Since the 1970s, while in practice a zone of intense conflict, French labor relations and labor law have focused on the notion of the enterprise as a community and employers and employees as citizens of that community with both rights and duties. Of course, what community meant to workers and employers was different. But both views stemmed from the measures seen as necessary for healing the scars of the political upheaval of 1968 and for heading off a left-wing victory at the polls in 1974.

For the worker, the enterprise community meant the workplace. This was a specific location where the employee's work and an extremely important network of social relations were found. Self-discovery and self-fulfillment were fundamental goals to be sought in the workplace in this social network. Like an echo of the demand for worker self-management of the 1960s, workers would come together in the workplace, form strong social bonds, and assert their collective power to create a community that served both their human and economic ends.

While the worker might subordinate herself to the employer by consent, that subordination was only for the purpose of performing work-related tasks. As stated in an influential 1992 report by the dean of French labor lawyers, Gerard Lyon-Caen, beyond the narrow confines of that subordination "in the rest of his life the worker


34. See id. at 102–3.
remains free . . . even during the execution of his work."  
Furthermore, Lyon-Caen argued, fundamental rights and liberties, particularly those that could be considered rights of personality, cannot be abrogated by the worker's consent or be alienated: "For his salary the worker exchanges services, which are defined by the employer, but which leave intact a core which corresponds, in a given epoch and a given civilization, to the idea of human liberty." In particular, this meant the liberty and the necessary conditions for French workers to form and maintain strong social bonds at work with their comrades and to act collectively to influence the organization and pace of work.

The enterprise community, for the employer, was a much more paternalistic concept. It stressed the role of the employer as the head of the community, while conceding the duty of the patron to limit such brutal and impersonal actions as mass layoffs and the duty to consult with workers prior to major changes in the work processes or terms of employment. In addition, for the first time, employers, hoping that this would give them more flexibility, recognized the legality of workplace union organization and the possible utility of collective agreements at the plant level. The employers assumed that the interest of the enterprise community, for which all should loyally strive, was the economic success of the business. The Socialist electoral victories of 1981 and the long tenure of Socialist President Mitterrand meant that the workers' viewpoint would have some influence over the law and jurisprudence.

The Italian Workers Statute of 1970, legislation also following a major political upheaval, the "hot summer" of 1969, affirmed even more strongly that the worker in the workplace enjoyed a right of personal dignity and an autonomous private sphere of action. According to influential Italian legal commentators, the rationale underlying the Workers Statute was that the worker at work remains a human being whose fundamental rights and human

36. See id.
37. Id.
38. See id. at 128.
39. See ROTHSTEIN, supra note 33, at 102.
40. See id. at 104–5.
dignity must be maintained. The notion of dignità humana in the workplace encompassed freedom of expression, autonomy and freedom from control by unidentified, impersonal or covert mechanisms. Article 4 of the Workers Statute, prohibiting the electronic surveillance of workers, arose from the idea that human dignity required that any monitoring of a person be undertaken by a person, not an impersonal machine. Monitoring, even by persons, must also be overt and not hidden, and proportional to a legitimate business end. Human dignity was preserved when the worker was able to confront the monitor, explain her activity to the monitor, understand the monitor's perspective and influence the monitor by collective action. Thus for the worker to maintain human dignity, she or he must be able to confront the human dignity of the monitor.

In France and Italy, unlike the U.S., there is legal recognition that private power is as much an attack on dignity and liberty as is public power. In the U.S., for example, certain protections related to privacy in the Fourth Amendment are held to apply only against government action. Furthermore, the trend with regard to public employment in the U.S. has been to reduce worker protections of privacy and autonomy to those found in the private sector. In France, on the other hand, the trend has been the reverse. The French Civil and Labor Codes now limit the restriction of constitutional rights and liberties by anyone (i.e. public or private persons). One French commentator has noted that the law "considers that the

43. See id. at 91–92.
44. See id. at 93–94.
45. See id. at 96–97, 99.
47. See Le Bris & Knopfers, supra note 28, at 422–23; PIERRE KAYSER, LA PROTECTION DE LA VIE PRIVÉE 77–78 (3d ed. 1995); Bennett, supra note 11, at 106–7.
49. See Hanson, supra note 49, at 248–57.
50. See KAYSER, supra note 47, at 19.
employee, although subordinated to the employer, always remains a free citizen whose fundamental rights do not disappear when he is at his job." Similarly, the Italian Workers Statute expressly refers to rights against government enshrined in the 1948 Constitution and applies them to workers in both the public and private sectors. Also, like the U.S. Constitution, it leaves much room for judicial interpretation.

IV. FRENCH LAW AND JURISPRUDENCE

In France the use of electronic technologies to monitor work activity is framed by three laws: the Law on Data Processing and Liberty, which regulates all automated treatments of data that identifies individuals; the 1970 amendment to Article 9 of the Civil Code protecting the right to respect for private life; and the 1992 amendments to the Labor Code for the protection of individual liberties in the enterprise. The 1992 amendments were a reaffirmation and an expansion to the workplace of the principles of the 1978 law and the 1981 Convention 108 of the Council of Europe. The protections for French workers are both procedural and substantive. Section L432-2-1 of the French Labor Code requires that employers inform and consult with the workers' council or other elected representatives of the workers in advance of any decision to put institute or modify methods of monitoring employees' activities, such as new technologies having important consequences for conditions of employment and data processing techniques related to personnel management.

The Labor Code has also applied the procedural requirements of the Law on Data Processing and Liberty to the workplace by requiring that an employee be informed in advance of any automated treatment of information identifying that employee and any automated techniques of professional

54. See Le Bris & Knopfers, *supra* note 28, at 430.
59. See C. TRAV. art. L.432-2-1.
evaluation. Where such information is collected, the employee must be advised whether the requested data is mandatory or optional; the employer must provide access to the data and the right to correct errant data. The new section L121-8 of the Labor Code specifies that no information concerning an employee or candidate for employment may be collected unless the employee is informed in advance of the means of collecting the data. The 1992 Law Aubry charged the Ministry of Labor's inspection division with seeing that the Law on Data Processing and Liberty was observed in the workplace by allowing the inspectors to investigate and bring a complaint to the CNIL or directly to local prosecutors.

The Law on Data Processing and Liberty of 1978 created the National Commission on Data Processing and Liberty (CNIL) as the guardian of fundamental rights affected by data processing techniques. The CNIL is charged with monitoring all automated treatments of data that identifies individuals. It studies, makes rules concerning, and approves applications for virtually all such treatments, public and private. The rules of the CNIL require, in advance of the installation or modification of an automated treatment of data that identifies individuals, the submission of a declaration describing the data and its treatment, the business purposes of the treatment, the procedures for informing interested parties, identification of those to whom the data will be transmitted, and the safeguards for protecting confidentiality. The CNIL also receives complaints, conducts field investigations and makes individual decisions concerning systems of data collection and treatment. Interestingly enough, despite these very broad powers, the operations of the CNIL are extremely independent of both the government and the business sector due to an unusual political deadlock and compromise at the time of its creation. It was created as the first French independent administrative agency. The power of appointment of most

60. See de Tissot, supra note 52, at 225.
61. See C.TRAV. art. L.121-8.
64. See id. at art. 6.
65. See id. at arts. 14–22.
66. See id. at art. 19.
67. See id. at art. 21; cf. CNIL, INFORMATIQUE ET LIBERTÉS: DOCUMENTATION GÉNÉRALE 4–6 (Doc. no. 36-15 1996).
68. See David H. Flaherty, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES, 172–74, 188–91 (1989); Interview with Alain Chouraqui, Labor Sociologist, L.E.S.T./C.N.R.S., Aix-
The substantive protections for workers from electronic monitoring and surveillance stem from the 1992 Law Aubry and to new life given to Art. 9 of the Civil Code by the courts. The new Art. 120-2 of the Labor Code, added by the Law Aubry, states simply: "No one may place restrictions on the rights of persons and individual or collective liberties which are not justified by the nature of the task to be accomplished and proportional to the objective sought." That sentence, borrowed from a provision of the Labor Code confined to work rules, introduces the notion that any restriction on individual or collective rights must be directly related to and proportional to the importance of a legitimate business interest. This notion is both broad and vague, leaving substantial room for judicial interpretation. Similarly, Article 9 of the Civil Code gives much leeway for judicial action. That article states: "Everyone has a right to respect for his private life. The judges may, without prejudice to compensation for injuries received, prescribe all measures, such as injunctions, seizures or other means, appropriate for preventing or halting an injury to the intimacy of private life; these measures, in an emergency, may be ordered summarily."

In the jurisprudential space created by these laws, the courts have been active. The French courts have several times rejected the use of tapes from hidden video cameras to prove the grounds for dismissal of an employee. One outstanding case found the French Supreme Court (Cour de Cassation) rejecting the dismissal of an employee where the evidence against the employee was the tape from a hidden video surveillance camera that showed the employee stealing from the register. The Court held that an employee...
may not be videotaped unless she or he is notified in advance of the taping and there are exceptional circumstances that justify the videotaping, e.g., repeated thefts.\textsuperscript{75} In another case, the Court of Appeals of Aix-en-Provence rejected videotape evidence of the negligence of a dismissed employee on the grounds that, given the easy availability of technologies to edit or forge images, the tape was unreliable as evidence.\textsuperscript{76}

In several cases, the courts have penalized employers for collecting or processing electronic data concerning employees without informing the employees in advance, consulting with the works council or submitting a declaration to the CNIL.\textsuperscript{77} The Paris Criminal Court fined the CEO and a data processing corporation for collecting and using performance statistics, attributable to identified employees, from the data entry stations of the operators.\textsuperscript{78} These statistics on numbers of keystrokes, numbers of corrections and times elapsed were posted daily in the work area and operators were evaluated and even dismissed based on the statistics.\textsuperscript{79} When a dismissed operator brought this to the attention of a Ministry of Labor Inspector, the Inspector investigated and obtained reinstatement for the employee.\textsuperscript{80} In addition the Inspector ascertained that the collection of these statistics was not the subject of notification or consultation with the employees or a submission to the CNIL, as the originally stated purpose was to collect aggregate—not individually identifiable—data concerning the operators.\textsuperscript{81} The case was brought to the local prosecutor resulting in a conviction for failure to declare to the CNIL a nominative treatment of electronically processed data and a fine of Fr 6000.\textsuperscript{82} While the law prescribes penalties of up to 3 years in prison and fines of up to Fr 200,000, the court's leniency was based on the fact that the collection of individually identifiable statistics stopped immediately upon the intervention of the Labor Inspector.\textsuperscript{83} Are French law and jurisprudence inspired by the idea of human

\textsuperscript{76} See Pérez c./SA Beli Intermarché, CA Aix-en-Provence, Jan. 4, 1994.
\textsuperscript{78} See Madame Arnoult c./Société SST, TC Paris (17e), Feb. 5, 1991, 1992 DROIT SOCIAL 541.
\textsuperscript{80} See id. at 540.
\textsuperscript{81} See id. at 540–41.
\textsuperscript{82} See id. at 541, 543.
\textsuperscript{83} See id. at 542.
dignity as suggested above? There are several important indications that the answer to this question is yes. The 1975 Report of the Commission on Data Processing and Liberty proposing the 1978 legislation discussed the threat to human rights, identity and dignity posed by means of collecting and treating personal data that are immeasurably more powerful and rapid than those available in the past. The first conclusion of the report was that an agency be created to serve as the “social conscience” of the nation with regard to the electronic collection and processing of personal data. Article I of the 1978 law states that data processing “shall infringe neither human identity nor the rights of man, nor private life, nor individual and public liberties.” While the language used in the legislation, and later European Community documents heavily influenced by the French example, stressed rights and liberties, these rights and liberties were seen as not only legal and individual, but moral and collective. The reference to “human identity” highlights an important element of human dignity. An influential study of the 1978 law noted that “the reference to human identity is a reflection of the concern over the homogenizing effect of data processing: over-generalization may harmfully limit human individuality. A case in point would be the characterization of an individual as a result of a few items of information.”

In the 1990s, concern that human dignity and identity were under attack received even greater emphasis in the annual reports of the CNIL. The increased use of new technologies for surveillance, monitoring and information collection and the demands of European integration were seen as a threat to the legal protections accorded French citizens through the work of the CNIL. The foreword to the 1992 report of the CNIL’s activities noted that the use of surveillance technologies touches not only a person’s liberties, but also her or his “identity itself.” It went on to note that if protections for citizens are reduced in the future, “mankind will be diminished.” The 1993 annual report warned of “the web which, with the advancement of technology, is woven little by little around each individual”

84. See 1 RAPPORT DE LA COMMISSION INFORMATIQUE ET LIBERTÉS 11–13 (1975).
85. See id. at 10.
87. See Le Bris & Knopfers, supra note 28, at 424.
88. Flaherty, supra note 68, at 178.
89. See BRAIBANT, supra note 68, at 41.
91. Id.
and which is changing "the conception one has of the individual and the society." Furthermore, the same section of the 1993 annual report noted:

But a new difficulty looms on the Atlantic horizon. How will the Americans, who have only embryonic protections [i.e., for individuals regarding the collection and dissemination of individually identifiable data], react commercially if Europe places conditions on the transborder flow of data that they cannot satisfy?

Even more clearly, the 1992 report to Minister of Labor Aubry, *Public Liberties and Employment*, authored by Gerard Lyon-Caen, advocated a greater emphasis on human dignity. The resulting Aubry Law seemed to accept this analysis. Lyon-Caen argued that the new technologies of data collection, treatment and surveillance had created a Foucauldian workplace where the employee was an object of measure rather than a person. Control was exercised internally to make the worker "transparent", thus robbing her of human dignity and identity. According to Lyon-Caen, this was far removed from the traditional and legal notions of subordination implied by the employment contract. Contributing to my argument regarding Italy as well as France, Lyon-Caen suggested that French labor law should more clearly affirm a right to personal dignity as did the Italian and Spanish worker statutes. This foundation was most important because it recognized the importance of and provided the protection for social relations in the workplace. This included real social relations with supervisors who were present and accessible as human beings.

With the implementation of the European Community Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Prime Minister Jospin commissioned

---

93. *Id.* at 7.
96. See *LYON-CAEN*, *supra* note 35, at 116.
97. See *id.* at 148, 158.
98. See *id.* at 117, 154.
99. *Id.* at 155.
100. *Id.* at 128–29, 156.
and received a report from the Conseil d'Etat (France’s Supreme Court for administrative law) which noted the emphasis of the Directive and French law on the protection of human dignity. The report warned of the dangers to human dignity of making decisions about individuals based only on quantified and computerized data about that individual and of the collection and transfer of individually identifiable data without the knowledge or consent of the identified person. Finally, the report contrasted the French and European data regulations designed to protect human dignity with the distinctly more limited American protections for privacy. Both the report and the Prime Minister have recommended the strengthening of the CNIL’s powers to regulate the collection, processing and use of personalized data.

V. ITALIAN LAW AND JURISPRUDENCE

The protection of workers from electronic monitoring is done differently in Italy. In France, as is typical in that highly bureaucratic, low-union-density country, the CNIL and the Ministry of Labor are charged with protecting the human dignity of workers from certain forms of data collection and electronic monitoring. However, the courts have provided some key interpretations of the law to bolster the authority of the agencies to protect workers against affronts to human dignity. The protections are written into specific laws and regulations and include the criminal law. In Italy, with a strong labor movement, creative jurisprudence has placed the protection of workers’ dignity from electronic monitoring more squarely in the hands of the unions.

Title I of the Italian Workers Statute of 1970, the preamble, is entitled “Of the Liberty and Dignity of the Worker.” Here the emphasis is on fundamental individual rights and liberties that are considered necessary for human dignity and act as limits on managerial prerogatives. These individual rights and liberties are securely established, however, in that they can

102. See Briabant, supra note 68, at 30, 45, 59.
103. See id. at 11–12.
104. See id. at 96–97.
106. See Ray & Rojot, supra note 32, at 71–73.
107. See Interview with Vincenzo Ferrante, Prof. of Labor Law, in Instituto Giuridico-CEDRI Università Cattolica de S.Cuore, Milan, Italy (Apr. 20, 1997) (on file with author).
effectively counter the power of an employer on a foundation of collective rights and the protection of trade union activities. The protection of workers against electronic surveillance and monitoring clearly shows this dual structure.109

The language of Article 4 of the Workers Statute prohibits remote surveillance of workers by video camera or other devices.110 Furthermore, the law does not allow an individual worker to consent to such surveillance. For reasons of business necessity, remote surveillance may be agreed to by union delegations or works councils.111 The individual worker may still have legal recourse to challenge the surveillance, even where the union has agreed, if the means used or the intensity is regarded by the Ministry of Labor or the courts as an infringement on human dignity.112 Article 4 clearly targets monitoring devices not directly related to the employee’s work, such as video and audio recordings.113 As a result, the installation of telephone accounting systems, computerized cafeteria inventories, safety monitoring devices and the electronic recording of sensitive banking and finance transactions have all required trade union agreement.114 Under the 1996 Italian law implementing the European Directive on personal data protection, the informed consent of each individual employee has been required before personally identifiable data may be transmitted by any organization that collects it.115 For example, the commission charged with administering this law116 has interpreted it to mean that an employer contracting with an outside accountant for payroll services needed the consent of each employee whose payroll data would be transmitted.117

The debate of the last fifteen years has been over the application of the Article to electronic monitoring that is made possible by the very equipment that the employee uses for her or his work, particularly computers or

109. See id. arts. 1, 4, 6 and 8; Spiros Simitis, Il diritto del lavoro e la riscoperta dell’individuo, 45 DLRI 87 (1990).
111. See id. at art. 4, para. 2.
112. See Romei & Sciarra, supra note 42, at 94.
113. See id. at 93.
114. Id. at 96–97.
116. Id. art. 30.
117. See Ferrante Interview, supra note 107.
computer-controlled machines. While Article 4 was originally drafted with the video surveillance of workers in a factory in mind, the language of the article included "other devices." Here the courts have followed the rationale of Article 4 to preserve the human dignity of the worker by preserving the human element in supervision and a reasonable amount of autonomy in the performance of the tasks required by the employment relationship. Generally the courts have prohibited the use of software installed for the purpose of minute and impersonal control of a worker's performance without prohibiting at the outset the introduction of equipment incidentally capable of exercising such control. For example, the courts since 1984 have consistently rejected the use of computer software that was designed to record elapsed time, mistakes, pauses and similar data on individual workers.

This debate began in earnest with a criminal case brought against several IBM Italy executives for violation of Article 4 of the Workers Statute in the Milan Criminal Court in 1982. The case, decided by the lower criminal court on December 5, 1984, gave rise to great controversy, appeals and an eventual settlement. In a lengthy opinion, the court struggled with Article 4's prohibition against remote monitoring of employees and with the penal sanctions imposed for violation of that Article by Article 38 of the same statute. The case concerned IBM's introduction of a computerized workflow analysis system called "Service Level Reporter" (SLR) designed for the collection of aggregate data on data processing operations. In collecting and aggregating data such as numbers of completed and aborted runs or mean elapsed times on batch jobs and runs, the system also collected and was capable of reporting data individually for each terminal used to submit a job. The identification of the terminal, of course, generally allowed the identification of the individual terminal operator. The evidence presented to the court by the IBM executives was that the evaluation of

118. See Romei, supra note 46, at 70.
119. See Ferrante Interview, supra note 107.
120. See Bellavista, supra note 46, at 209–10.
121. See Romei & Sciarra, supra note 42, at 93–94.
122. See Bellavista, supra note 46, at 209–10.
124. See Ferrante Interview, supra note 107.
127. See id. at 210–11.
individual employee's work was not the purpose for which the system was installed nor was a report of such individual information ever requested or used for employee evaluation. The case then turned on whether a system which could potentially be used for the remote monitoring of individual workers, but was not intended to be so used and was in fact not so used, gave rise to the penal sanctions of Article 38.

The court relied heavily on the distinction between the language of paragraph one and paragraph two of Article 4. Paragraph one states: "It shall be unlawful to use videocameras and other equipment for the remote monitoring of workers' activity." Paragraph two refers to "[c]ontrol equipment and appliances required for organisational [sic] and productive reasons or for work safety but which could be used for the remote monitoring of workers...." This latter category of equipment "may be installed only after obtaining the agreement of the trade union delegations or, failing this, that of the works council." The court took for granted that this provision included the installation of software as well as hardware.

The court reasoned that the legislative intention behind paragraph one was the outright prohibition, subject to criminal sanction, of the installation or use of remote-surveillance equipment not directly connected to the firm's productive purposes or the employees' work. This would include such equipment as video surveillance devices, audio listening devices and magnetic badges for tracking the whereabouts of employees. This type of equipment, the court found, directly infringed upon the dignity and autonomy of the worker by subjecting her to constant, impersonal monitoring of her actions.

Paragraph two, on the other hand, dealt with the installation of equipment that at the outset was directly related to the firm's productive purposes and to the work of the employees and was only potentially capable of the remote monitoring of the employees' actions on an individually

128. See id. at 212–13.
129. See id. at 214.
131. Id. art. 4, para. 2.
132. Id.
134. See id. at 216, 230.
135. See Romei, supra note 46, at 72.
That equipment was subject to certain conditions limiting its use that could allow its installation. Here the court tried to balance the employer’s interest in the use of equipment that was essential to the work being done and that monitored work processes for the purpose of improving their efficiency with the employees’ interest in the protection of their human dignity and autonomy.

For several reasons the court found the proof of the IBM officials’ criminal culpability insufficient. In the first instance, at the time of the installation of the computer terminals, the potential of remote monitoring of individual employees was too speculative and outside of the use intended by the responsible IBM officials to fall under the prohibitions of Article 4. The installation of the SLR system software, however, did fall within those prohibitions. However, the imposition of criminal liability required knowledge of the system’s capabilities for individual employee monitoring and intent to make use of them, the best evidence of the two elements being the actual use for individual monitoring. Second, even if the IBM executives had some knowledge of the system’s potential, a partial agreement on some aspects of computerized data collection on, and monitoring of, individual employees had been reached in early 1982 with the local trade union delegation. The court reasoned that although this agreement might ultimately be found to be insufficient to cover, or breached by, the installation of the SLR system, it did throw further doubt on the criminal knowledge and intent necessary for imposing penal sanctions on the IBM executives.

In the end the court acquitted the officials on the criminal charges while expressly noting the possibility of a successful civil action. In its opinion the court recognized that the computerized monitoring of an employee’s activities for the purpose of evaluating an individual employee’s work was an assault on that employee’s human dignity even where the monitoring was done by a machine necessary for the employee’s work. Human dignity required that an employee not be subjected to the impersonal, mechanical,

137. See id. at 229–30.
138. See id. at 231–35.
139. See id. at 238–39.
140. See id. at 240–41.
141. See id. at 241–43.
142. See id. at 243–44.
143. See id. at 245–48.
144. See id. at 252.
145. See id. at 222–23.
and constant surveillance of a machine and that an employee not be evaluated impersonally by electronically processed quantitative data alone.\textsuperscript{146} The autonomy necessary for protecting human dignity required that an employee participate in collective decisions about the monitoring and evaluation of his or her work.\textsuperscript{147}

Ultimately the case was settled based on an extension of the 1982 agreement whereby the company agreed not to collect data attributable to individual operators except where that data was critical to the operation of the business.\textsuperscript{148} The designation of individually identifiable data critical to business operations would be the subject of a joint examination by the employer and the union on a case-by-case basis.\textsuperscript{149}

As later court cases and commentators have reaffirmed, the basis for Italian law on the electronic monitoring of workers is that supervision must have a human dimension and must not be so powerful, continuous, anonymous, invisible or inflexible as to eliminate a considerable measure of autonomy or reserve in the employee’s performance of a task.\textsuperscript{150} In addition, supervision must be directly related to the tasks required of the employee and not disproportional in intensity to the nature and importance of those tasks.\textsuperscript{151} Furthermore, the main assurance that these limits are observed by the employer is the intervention of trade union representatives in the decision making concerning techniques of supervision.\textsuperscript{152} Italian jurisprudence has established these as central elements of the protection of human dignity in the workplace.\textsuperscript{153}

\textbf{VI. AMERICAN LAW AND JURISPRUDENCE}

\textit{A. Federal Law}

In contrast, the limitations in the United States on an employer’s use of electronic surveillance and monitoring techniques, based on a narrower

\begin{itemize}
  \item \textsuperscript{146} See \textit{id.} at 224.
  \item \textsuperscript{147} See \textit{id.} at 225.
  \item \textsuperscript{148} See \textit{id.} at 241; \textit{Accordo IBM-SEMEA, Milano e RSA}, Feb. 23, 1982.
  \item \textsuperscript{149} See Interview with Chief of Personnel, IBM-SEMEA, Milan (Jan. 7, 1998) (on file with author).
  \item \textsuperscript{150} See Mariella Magnani, \textit{Diritti della persona e contratto di lavoro: L’esperienza Italiana}, 15 QUADERNI DI DIRITTO DEL LAVORO E DELLE RELAZIONI INDUSTRIALI 47, 53 (1994); \textit{Bellavista, supra} note 46, at 198.
  \item \textsuperscript{151} See \textit{Romei & Sciarra, supra} note 41, at 96–97.
  \item \textsuperscript{152} See \textit{id.} at 91.
  \item \textsuperscript{153} See \textit{Magnani, supra} note 150, at 50–51.
\end{itemize}
concept of protecting a worker’s privacy rather than human dignity, are much less extensive.\textsuperscript{154} There are several putative sources of the legal protection of workers from electronic surveillance and monitoring in the workplace; on close investigation, however, these sources provide little protection.\textsuperscript{155} The “usual suspects” for generating privacy protection in the workplace are the Fourth Amendment’s protection from unreasonable searches and seizures,\textsuperscript{156} the federal Electronic Communications Privacy Act,\textsuperscript{157} state constitutions and statutes protecting privacy or barring specific means of surveillance,\textsuperscript{158} and common law remedies for invasion of privacy or abusive discharge.\textsuperscript{159} Of course, a collective bargaining agreement could explicitly limit the monitoring of employees, but both practical and legal difficulties exist that make this rare. To a certain extent both American workers and their employers begin with a legal concept of privacy that is much narrower than the Europeans’ (at least the workers’) notion of human dignity. The territory- and property-oriented concept of privacy that is pervasive in American law cedes to the employer, the owner of the work premises and equipment, and the imposer of the terms of employment, a wide latitude in the content and the means of gathering information about the employees’ activities in the workplace and beyond.

Let us consider the “usual suspects” mentioned above in order. The Fourth Amendment to the U.S. Constitution guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”\textsuperscript{160} The Supreme Court has acknowledged that this right may apply to the electronic gathering of

\textsuperscript{154} See Schwartz, supra note 11, at 408; Mark A. Rothstein, Genetic Secrets: A Policy Framework, in GENETIC SECRETS, 454 (Mark A. Rothstein ed. 1997).


\textsuperscript{156} See U.S. CONST. amend. IV.


\textsuperscript{159} See, e.g., cases dealing with the surveillance of workers after they filed work injury claims such as: Johnson v. Corporate Special Serv., Inc., 602 So.2d 385, 386 (Ala. 1992) and Alabama Elec. Cooper. v. Partridge, 225 So.2d 848, 851 (Ala. 1969).

\textsuperscript{160} U.S. CONST., amend. IV § 1.
information and to employment situations.\textsuperscript{161} However, this right is only protected against government action: the Fourth Amendment establishes no right against unreasonable searches and seizures by private employers.\textsuperscript{162} As a result government employees may appear to have a somewhat stronger claim for protection against electronic monitoring and surveillance than private sector employees. This difference is illusory. To a large extent, private employment law analogies have entered into the key legal determination of whether the government employee has a "reasonable expectation of privacy" regarding the workplace or activity in question.\textsuperscript{163} The government employer's control of the premises and the equipment, the implied consent of the worker who is generally informed that monitoring might take place and the balancing of the magnitude of the intrusion into the employee's control over personal intimacy or information against the business necessities and efficiency of the public employer all combine to greatly limit a government employee's "reasonable expectation of privacy."\textsuperscript{164}

In \textit{O'Connor v. Ortega}, a case regarding the physical search of an employee's desk, Justice O'Connor's plurality opinion held that an employee's expectation of privacy is limited by "actual office practices" and "legitimate regulation,"\textsuperscript{165} that is to say, if monitoring or surveillance were existing practices known to the employee or the employer had a stated policy of random or regular surveillance, the employee's expectation of privacy would be defeated. This clearly leaves the determination of the employee's reasonable expectation of privacy solely in the hands of the government employer. The plurality opinion went on to say that a non-investigatory work-related search is presumed to be reasonable.\textsuperscript{166}

Furthermore, the work-related reason for the surveillance or search need not be an important reason and it may be one of many reasons, even though the others, standing alone, would render the search or surveillance improper.\textsuperscript{167} It is unlikely then that any apparently work-related reason will be rejected by a court as the justification for surveillance and monitoring. In general, courts have not required that the government employer prove the

\begin{itemize}
\item \textsuperscript{163} See \textit{O'Connor}, 480 U.S. at 717.
\item \textsuperscript{164} See \textit{Hanson}, \textit{supra} note 48, at 249–51; \textit{Gantt, supra} note 31, at 385.
\item \textsuperscript{165} See \textit{O'Connor}, 480 U.S. at 717.
\item \textsuperscript{166} See \textit{id.} at 726.
\item \textsuperscript{167} See \textit{e.g.}, \textit{Diaz Camacho v. Lopez Rivera}, 699 F. Supp. 1020, 1024–25 (D.P.R. 1988).
\end{itemize}
actual existence or validity of an alleged work-related purpose for a search or surveillance. The burden is on the employee to show that an allegedly work-related search or type of monitoring was clearly unreasonable under existing law. The Fourth Amendment, enmeshed in the privacy context, clearly does not address questions of the intensity or impersonality of the surveillance. Tied to the "state action" requirement, the Fourth Amendment and its extension through the Fourteenth Amendment do not affect private employment.

The Electronic Communications Privacy Act of 1986, ("ECPA") which updated the Wiretap Act to cover private communications systems and new forms of electronic communication that were not telephone, telegraph or radio transmissions, has generally proven ineffective in protecting employees in the workplace from their employers' monitoring. The ECPA would seem to have particular relevance to the monitoring of phone calls and email at work in that it prohibits the interception of data transmitted by wire, radio or other electronic means. There are, however, three major exceptions to the prohibition which give employers virtually a free hand to engage in such monitoring.

Provisions of the ECPA establish a "provider" exception. These provisions allow the provider of a private communication system or its employees or agents to monitor the use of its equipment. When the employer provides the equipment and/or the network, or can be seen as the agent of the provider, monitoring telephone calls and electronic communications remains generally legal. However, there are exceptions to this rule that allow for greater employee protection.


172. See Wilborn, supra note 48, at 839–40.


175. See id. The statute exempts an officer, agent or employee of a provider of a "wire or electronic communication service, whose facilities are used in transmission of a wire communication..." Id.
communications of its employees, at least where the employer deems it necessary to protect the business or insure the proper use of the communication equipment, falls into this exception.\textsuperscript{176}

There is also a business extension exception which removes from the definition of “device” any telephone or component “furnished to the subscriber or user by a provider of [the] ... communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business ...”.\textsuperscript{177} If the monitoring of calls, voice mail or email is for the purpose of supervision, evaluation or any other asserted business interest of the employer, the monitoring is permissible under this exception.\textsuperscript{178} This generally includes as well the interception of non-business-related employee communications at least to the extent necessary to determine that they are such or to determine that the equipment is being used in an unauthorized manner.\textsuperscript{179} If a personal call mentions workplace activities in any way, it may again fall into the ordinary course of business exception.\textsuperscript{180}

Furthermore, the ECPA excludes any recording or interception of communications where one of the parties to the communication agrees to the recording or interception.\textsuperscript{181} The “agreement” to have one’s communications monitored may be general and implicit.\textsuperscript{182} Here again the employer sets the standards.\textsuperscript{183} If there is an established policy of monitoring or the employee is at least aware that monitoring may occur, then initial and continued employment can be seen as consent to the monitoring.\textsuperscript{184} Of course, in an at-will employment situation, the employee may be dismissed for refusing to agree to monitoring.\textsuperscript{185} If a party to the communication other than the

\begin{footnotesize}
\textsuperscript{176} See \textit{id}. It goes on to state that the exempted provider may “intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.” \textit{Cf.} Lois R. Witt, \textit{Terminally Nosy: Employers Free to Access our Electronic Mail?}, 96 DICK. L. REV. 545, 551 (1992).


\textsuperscript{178} See James v. Newspaper Agency Corp., 591 F.2d 579, 581 (10\textsuperscript{th} Cir. 1979).

\textsuperscript{179} See Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11\textsuperscript{th} Cir. 1983).


\textsuperscript{182} See Griggs-Ryan v. Connelly, 904 F.2d 112, 116, 117 (1\textsuperscript{st} Cir. 1990).

\textsuperscript{183} See Watkins, 704 F.2d at 581–82.

\textsuperscript{184} See George v. Carusone, 849 F. Supp. 159, 163 (D. Conn. 1994); \textit{but see} Deal v. Spears, 980 F.2d 1153, 1157 (8\textsuperscript{th} Cir. 1992).

\end{footnotesize}
employee under surveillance agrees to the monitoring, there need be no knowledge or consent of the employee.\textsuperscript{186}

If the employee were to store electronic communications on her office PC hard disk or network storage provided by the employer, the employer would not be in violation of the ECPA if she searched these storage sites and read the messages.\textsuperscript{187} The only electronic storage the ECPA protects is defined as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."\textsuperscript{188} Overall court interpretations and commentators on the ECPA have not regarded it as an important protection for workers in the workplace.\textsuperscript{189} Indeed, the legislative history of the ECPA reflects concern for company privacy rather than that of individual employees.\textsuperscript{190}

In an interesting counterpoint that highlights the European-U.S. difference, Northern Telecom settled a lawsuit with its union, the Communications Workers of America, over the secret electronic monitoring of employee communications over a thirteen year period. Northern Telecom renounced its monitoring policy, noting that in Japan and Europe such monitoring was already banned with no detrimental effect on business performance.\textsuperscript{191}

\begin{flushright}
\textsuperscript{189} For cases, see supra notes 179–80, 183–85; for commentators, see infra note 190.
\end{flushright}
While several states have constitutional provisions guaranteeing a right to privacy, only one state, California, has held that the right to privacy applies to private as well as governmental employers. The employer must show a "compelling interest" to justify an intrusion upon the employees right to privacy. However, the California Superior Court, in Flanagan v. Epson America, refused to apply the right to privacy to a private employee's e-mail. The court suggested that the extension of constitutional privacy rights was for the legislature, not the judiciary.

Forty-eight states and the District of Columbia have statutes similar to the federal ECPA, prohibiting the interception of electronic communications. Many of these states echo the one party consent, "business extension" and "provider" exemptions of the ECPA. Thirteen states require that prior consent must be given by all parties to the communication. Twenty-two states and Washington, D.C. have no "business extension" exception or restrict the "provider" exception to communication common carriers. In thirty-one states and D.C., therefore, the electronic communication privacy statutes seem to provide protection for employees superior to the ECPA as long as the interception occurs within the workplace.

192. See Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 641 (Cal. 1994); Porten v. Univ. of S. F., 134 Cal. Rptr. 839 (1976); Semore v. Pool, 266 Cal. Rptr. 280 ( Ct. App. 1990), reh. den. 5 I.E.R. Cas. (BNA) 672 (1990). See also Conlon, supra note 155, at 287; Wilborn, supra note 48, at n.65; Lee, supra note 190, at 144.


195. See Flanagan, slip op. at 4.

196. The only states that do not have such statutes are South Carolina and Vermont.


198. These jurisdictions are Alabama, Delaware, the District of Columbia, Georgia, Idaho, Indiana, Iowa, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Missouri, New Hampshire, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, and Texas.
their jurisdiction.\textsuperscript{199} This appearance is deceptive. The Illinois courts, for example, have interpreted the apparent all-party consent requirement to mean at least one party.\textsuperscript{200} As all of the states are also at-will employment states, the implied consent of all employee participants in a communication is assumed in most cases. Furthermore, while these statutes apply to the monitoring of telephone and wire communications, they do not reach other forms of electronic monitoring and surveillance. State bills to strengthen the protections of workers against electronic monitoring in the workplace have generally failed because of sustained and effective corporate lobbying.\textsuperscript{201}

The Restatement (Second) of Torts, the definitive treatment of state common law regarding privacy recognizes "the unreasonable intrusion into a person's seclusion"\textsuperscript{202} as the sole relevant basis for establishing privacy rights in the workplace. These words themselves seem immediately inappropriate for the workplace where a person is on the premises owned by another and in the presence of co-workers and the employer. The intrusion claim implies an unreasonable and objectionable prying into something one has a right to keep private. Outside of the employment setting there are two independent considerations: (1) Did the individual intruded upon have a legitimate expectation of privacy?; (2) Did the legally protected interests of the intruder outweigh the legitimate expectation of privacy? When the claim is moved into the employment arena, courts have conflated the two considerations, allowing the employer's interests to dominate.\textsuperscript{203} The employer may unilaterally change the employee's expectation of privacy by instituting a policy of intrusion or by simply intruding on one or more occasions. As the employer has the right to manage the employee for the employer's business purposes, there is little that the employee has a right to keep private if it impinges in any way on the workplace.\textsuperscript{204} The employee consents to any intrusions by remaining at work after becoming aware of the intrusion or the possibility of such an intrusion.\textsuperscript{205} Finally, an at-will

\begin{itemize}
\item \textsuperscript{199} See Conlon, \textit{supra} note 155, at 289; Lee, \textit{supra} note 191, at Table 2.
\item \textsuperscript{201} See Lee, \textit{supra} note 190, at 146. On lobbying over privacy concerns, see generally Matthew W. Finkin, \textit{The Kenneth M. Piper Lecture: Employee Privacy, American Values and the Law}, 72 CHI.-KENT L. REV. 221, 224 (1996).
\item \textsuperscript{202} \textit{RESTATEMENT (SECOND) OF TORTS} § 652A (1977).
\item \textsuperscript{204} See Finkin, \textit{supra} note 201, at 256.
\end{itemize}
employee who objects to the intrusions or the policies allowing them may be immediately dismissed.206

_Smyth v. Pillsbury_207 clearly takes up and severely restricts any common law right to privacy of e-mail communications for an at-will employee. Smyth claimed that he was wrongfully discharged from his position as regional operations manager when Pillsbury discharged him for sending sarcastic and critical e-mail communications to his supervisor.208 Smyth had received e-mail communications sent from his supervisor’s computer at Pillsbury to Smyth’s home computer. The two employees then exchanged e-mail communications concerning recent developments involving Pillsbury’s sales management staff.209 The supervisor deemed Smyth’s comments inappropriate.210 The _Smyth_ court held that an at-will employee had no right of privacy in the contents of his or her e-mail when it was sent over the employer’s e-mail system.211 The court concluded that, in a Pennsylvania common law cause of action for wrongful discharge, an at-will employee does not have a reasonable expectation of privacy in the contents of his e-mail communications sent through his employer’s e-mail system.212 The court held further that an employer’s interest in preventing inappropriate comments or illegal activity from being transmitted over its e-mail system far outweighs any privacy interest an employee may have in his e-mail communications.213 While the court seemed to take a strained and unsophisticated view of the issues at stake, it provided the most recent statement on the extreme difficulty of protecting workers by means of any U.S. common law of privacy.214

With regard to computer-based surveillance, in _Barksdale v. IBM Corp._, the court dismissed short-term employees’ claims of violation of the right to privacy stating that “[t]he Defendant’s observation and recording of the number of errors the Plaintiffs made in tasks they were instructed to perform can hardly be considered an intrusion upon the Plaintiff’s ‘solitude or

208. See id. at 98.
209. See id. at 98–99.
210. See id. at 99.
211. See id. at 101.
212. See id.
213. See id.
214. See generally Dixon, supra note 190. See also Finkin, supra note 201, at 227–28; Lehman, supra note 190, at 105–7.
seclusion... or their private affairs and concerns." While this was an unusual case because of the short-term nature of the employment and the job of testing the visibility of computer monitors, it still made clear that the employer defined the reasonableness of the employees' expectations of privacy by the nature of the tasks he assigned and the practices he followed.

VII. CONCLUSION: OTHER NOTIONS OF PRIVACY THAT BORDER ON HUMAN DIGNITY

The foregoing analysis of the deficiencies of the U.S. legal concept of privacy in the workplace as a protection against electronic surveillance does not preclude the fact that there have been attempts in the U.S. legal culture to develop a more comprehensive notion of privacy that would have some of the impact of notions of human dignity and autonomy. The Prosser/Restatement of Torts view of privacy that dominates U.S. law has not gone unchallenged in the American legal community. Edward Bloustein argued compellingly in direct response to Prosser's seminal 1960 article that Prosser and American courts have misconstrued the very founders of the common law right to privacy in the U.S., Samuel Warren and Louis Brandeis. Bloustein noted that their 1890 Harvard Law Review article was very clear on the point that the right to privacy derived, not from notions of private property (as courts have declared), "but that of inviolate personality." Bloustein concluded this meant, "the individual's independence, dignity, and integrity; it defines man's essence as a unique and self-determining being." And as had Warren and Brandeis, Bloustein in the end warned that

The personnel practices of government and large-scale corporate enterprise increasingly involve novel forms of investigation of personal lives... And the information so gathered is very often stored, correlated and retrieved by electronic machine techniques.

218. Id. at 205.
The combined force of the new techniques for uncovering personal intimacies and the new techniques of electronic use of this personal data threatens to uncover inmost thoughts and feelings.\textsuperscript{220}

In another frequently quoted article, Ruth Gavison stated:

Our interest in privacy . . . is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur. Furthermore, the reasons for which we claim privacy in different situations are similar. They are related to the functions privacy has in our lives: the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society. The coherence of privacy as a concept and the similarity of the reasons for regarding losses of privacy as undesirable support the notion that the legal system should make an explicit commitment to privacy as a value that should be considered in reaching legal results.\textsuperscript{221}

The explicit recognition of the broad concept of privacy Gavison recommends would give an employee's privacy claims regarding employer collected data much greater weight in any balancing against the employer's interest in the efficiency of his business operations. Courts very rarely seem to accept this expanded notion of privacy. In a very few cases dealing with the "telephone extension" and "ordinary course of business" exceptions to the ECPA have held that excessive monitoring by employers, particularly if covert, may lead to ECPA violations.\textsuperscript{222}

But as James Rule and his colleagues noted in The Politics of Privacy, this balancing in itself may be the problem. Privacy and data protection laws frame the issues too narrowly. While public policies that seek to "balance" privacy rights with organizational demands for information may produce a fairer and more efficient management of personal data, they cannot control the growing inherent demand and technological capacity of bureaucratic

\textsuperscript{220} Id. at 191.
\textsuperscript{221} Ruth Gavison, Privacy and the Limits of Law, 89 YALE L.J. 421, 423–4 (1980).
\textsuperscript{222} See e.g. Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994); Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); United States v. Harpel, 493 F.2d 346 (10th Cir. 1974); James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979).
institutions to gather, store and access detailed personal information. Against this, policies of outright prohibition of specific technologies and of gathering certain kinds of data may be the only answer, however temporary.

Several legislative bodies have unsuccessfully attempted to control electronic monitoring in the workplace based upon a much broader notion of privacy that encompassed human dignity. The foremost was the Privacy for Consumers and Workers Act of 1993 ("PWCA"). Supporters of the bill argued that the technocrats who designed workplace surveillance systems had forgotten the humanity of employees. If the technology slices people up into tiny pieces and views them under a microscope, their spirit is destroyed. They argued that the bill would take steps toward treating employees with respect and dignity. The bill defined electronic monitoring broadly:

[T]he collection, storage, analysis, or reporting of information concerning an individual's activities by means of a computer, electronic observation and supervision, 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.

Section 4 of the bill required an employer to provide a prior written notice to each employee to be monitored. The notice had to describe the forms of electronic monitoring to be used, the personal data to be collected, and the hours and days that monitoring would occur. The employer also

---

227. See id.
228. S. 984, 103rd Cong. § 2(1)(A) (1993).
229. See id. at § 4(b).
230. See id. at § 4(b)(1)–(3).
was required to explain how the data obtained would be used and provide a description of the monitoring. Furthermore, the same section required the employer to inform prospective employees in writing of existing forms of monitoring.

Section 5 of the bill permitted unlimited random monitoring of employees only in the first sixty days of employment. For employees with less than five years and greater than sixty days of employment, random monitoring could not exceed two hours per week. Monitoring of workers with at least five years employment in the enterprise was prohibited, except in cases of suspicion of criminal activity or of gross misconduct damaging to the business.

Section 8 of the bill prohibited the employer from taking any action against an employee based on the personal data obtained by electronic monitoring unless the employer was in compliance with all requirements of the PCWA. Nor could an employer use quantitative data obtained by monitoring that records the amount of work performed by an employee within a specific time as the sole basis for individual employee performance evaluation or to set production quotas or work performance expectations. If an employer had an immediate need for specific data while the employee concerned was unavailable, the employer could access the data if it was alphanumeric and was not an employee communication, so long as the data was not used for employee discipline or performance evaluation, and the employer notified the concerned employee of his access to the information.

Additional provisions prohibited electronic monitoring in bathrooms, locker rooms, or dressing rooms unless the employer has a reasonable suspicion that an employee was engaged in unlawful activity and prohibited the intentional use or dissemination of personal data obtained by electronic monitoring of an employee when the employee was exercising First Amendment rights.

231. See id. at § 4(b)(4)–(5), (8).
232. See id. at § 4(c)(2).
233. See id. at § 5(b)(1).
234. See id. at § 5(b)(2).
235. See id. at § 5(b)(3).
236. See id. at § 8(a).
237. See id. at § 8(b)(1)–(2).
238. See id. at § 9(a)(1)–(3).
239. See id. at § 9(b)(B)(1)–(3).
240. See id. at § 9(c)(1).
Similar unsuccessful legislation proposed in Massachusetts and effectively resisted by business interests specified the rights it sought to advance in this manner:

1) Right to Know: Employees have the right to know if, when, and how they are being monitored along with how the information gathered will be used.
2) Right to Privacy: Employees should be protected from monitoring that is irrelevant to job performance.
3) Right to Due Process: Employees have access rights to information collected through monitoring, and must be given access to the information in a timely manner if the information is to be used against them.
4) Right to Human Dignity: Employees have the right to be evaluated by means other than electronic monitoring, because a human side to every job exists which cannot be evaluated electronically.\(^{241}\)

In West Virginia a statute prohibiting secret telephone monitoring was passed in 1981.\(^{242}\) AT&T, which had engaged extensively in such monitoring prior to the passage of the statute, was forced to discontinue its secret monitoring of telephone operators responses to customers.\(^{243}\) Even though during the two years following the passage of the law, the West Virginia AT&T division was rated outstanding in the Bell System on customer service, the company successfully lobbied for the repeal of the legislation in 1983.\(^{244}\) AT&T’s lobbying efforts included the threat not to locate a planned major manufacturing facility in West Virginia.\(^{245}\)

The failure of these pieces of legislation makes clear that the incorporation in U.S. law of a broader notion of privacy which includes human dignity is strongly resisted. The West Virginia legislation, the PCWA and the Massachusetts bill were implacably opposed by business interests.


\(^{242}\) See Hearing on S. 984 Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor and Human Resources, 103rd Cong. 21 (1993).

\(^{243}\) See id.

\(^{244}\) See id.

\(^{245}\) See id.
and that opposition led to their repeal or defeat.\textsuperscript{246} Although a change in the composition of Congress might lead to the revival of the PCWA or a similar bill, its passage would still be questionable. Likewise, as the foregoing analysis has attempted to show, American jurisprudence has not broadened the notion of privacy for the protection of workers' autonomy from overly intense or highly impersonal forms of supervision. This expanded notion of privacy does not seem to be a logical extension of the Prosser definition of the tort of invasion of privacy. It may, therefore, be strategically wise for those who advocate an extension of worker autonomy and restrictions on subordination in the workplace to attempt to move the debate to a notion of human dignity that must be protected wherever a person is and whoever defines the tasks that must be performed. In addition, human dignity as a value is much more closely related to collective action and to the sharing of decision-making power and thus more in tune with the purposes and actions of labor unions to protect workers. Privacy, on the other hand, implies the protection of solely individual interests against all others. An emphasis on human dignity may lead to policies that reflect the higher standards of worker protection and participation existing in French and Italian law.

\textsuperscript{246} See id., Baxi & Nickel, supra note 241, and Note, supra note 241.