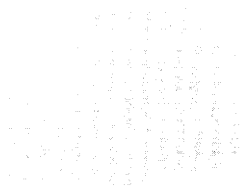
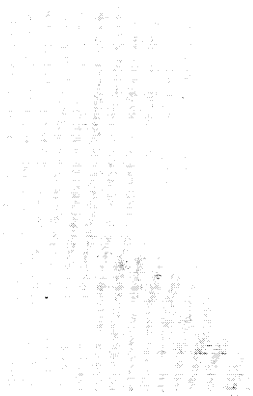
Chapter

Electronic Work Monitoring Law and Policy Considerations





CONTENTS

Tables

Chapter 4

Electronic Work Monitoring Law and Policy Considerations

With perhaps the exception of marriage, no other institution in society is so pervasive as the employment relationship.[1] Roughly half of an adult waking hours are spent at work. Societal attitudes regarding personal dignity, autonomy, and privacy, and the individual's sense of self are tied to the workplace. Electronic monitoring-the computerized collection, storage, analysis, and reporting of information about employees' productive activity[2] —may be an increasingly important element in the relationship between employer and employee, and in the overall context in which work gets done. Decisions about monitoring may affect the setting in which citizens work, and may therefore have a broader social significance.

Between 4 and 6 million office workers have their work measured by computers, and many millions more are affected by telephone call accounting.[3] Proponents of electronic monitoring, principally the vendors of monitoring equipment and software and some companies that have installed monitoring systems, say that monitoring provides employers with new tools for managing resources, allocating costs, improving productivity, controlling quality, and reducing waste, fraud, and abuse of employer property. At the same time, however, critics of work monitoring, principally some labor unions and civil liberties organizations, suggest that electronic work monitoring is destructive to the quality of work life and has damaging effects on workers' privacy, civil liberties, sense of dignity, and health.

This chapter is an attempt to provide the policy maker with a conceptual framework for addressing concerns over electronic monitoring, now and in the future. It begins by asking why monitoring has become a policy issue, and what is different about *electronic* monitoring that causes these concerns. It then examines which of these concerns are currently addressed by existing law and which are not. Finally, it provides the policy maker with a range of options from which to choose.

[1]See ch. 2.

"We have become a nation of employees . For our generation, the substance of life is in another mans hands." F. Tannenbaum. *A Philosophy of labor* 9 (1951) (as quoted in Blades, "Employment at Will vs. Individual Freedom: On Limiting the Abusive Exercise of Employer Power," 67 *Columbia Law Review* 1404 (1967). Although the employment relationship is freely entered into, the need to earn a living, together with limitations the individual's qualifications and the ease with which he or she can be substituted, often place the worker at a disadvantage in determining the conditions under which he or she shall work.

"'Electronic work monitoring," "electronic monitoring," or just "work monitoring" are terms used interchangeably in this chapter and elsewhere in this report to include computer-based work monitoring and telephone service observation. Telephone service observation, although not typically computerized, is included because it is often used in conjunction with electronic work measurement techniques.

PART I: WHY IS MONITORING AN ISSUE?

Neither work monitoring, nor the application of technology to measure work, is new. As chapter 1 of this report illustrates, the detailed observation and recording of employee performance has been an integral part of American industrialization from the mid-1800s onward. During the early 1900s, work monitoring culminated in Frederick W. Taylor's "scientific management. While early work monitoring techniques were confined to pencil and paper tallies of performance, technologies such as the time clock, time stamps, and cyclometers were applied pervasively to the measurement of work.[4]

[1]For a more complete discussion of early forms of work monitoring, see ch. 1 of this report.

Given this long history of work monitoring, two questions arise:

1. why is concern about work monitoring among management, labor, and public interest groups only now surfacing? and
2. why is the application of electronics to an old-technique unique or different enough to cause this concern?

Simply put, the questions are "why now?" and "what new?" The first question is addressed presently, while the second forms the discussion in the remainder of this chapter.

Although the question of "why now?" has no simple answer, it is possible to point to three broad trends that have contributed to the emergence of monitoring as a policy issue: the computerization of office work, the computerization of communications, and the rise of workers' expectations and rights in the workplace. The three types of monitoring considered in this report—computer-based monitoring, telephone call accounting, and telephone service observation—illustrate the way in which these trends have propelled work monitoring into the national policy arena.

The computerization of office work is less than 15 years old—less than half of the working lifetime of a white-collar worker.[5] Computerization has lead to rapid, fundamental changes in the quantity, quality, and organization of office work. As a result, conflicts are emerging between management and labor over how work will be designed; who will have a say in that design; and what the expectations of employee performance, flexibility, and privacy should be. The literature on the impact of automation on work is voluminous, and the reader seeking more information is referred to another OTA report, *Automation of America Offices.*[6]

Computer-based monitoring is one example of how the computerization of office work has lead to the recent emergence of work monitoring as a salient issue. Since 1982, computer-based monitoring has been the subject of national TV news programs, a stream of newspaper and magazine stories, and several recent books. Although it has captured media attention, unions were the first principal critics of computer-based monitoring.[7] (Unions having positions against computer-based monitoring are listed in table 11). While the concerns of each union are not necessarily identical in details, a broad consensus seems to be that work speedups, enforced by close work monitoring, are bad because they create harmful *stress* among employees and also compromise the

Table 11.—20 Unions With Positions Against Computer-Based Work Monitoring

Union	Estimated membership
Automobile, aerospace, and agricultural workers (UAW)	**1,350,000**
Communications workers (CWA)	**550,000**
Electrical workers	1,000,000
Electronic, electrical, technical, salaried, and machine workers (IUE)	160,000
Federal employees (NFFE)	150,000
Government employees (AFGE)	265,000
Government employees (NAGE)	300,000
Machinists (IAM)	940,000
Newspaper guild (TNG)	40,000
Office and professional employees (OPEU)	125,000
Postal workers (APWU)	320,000
Railway, airlines, and steamship clerks (BRAC)	200,000
Service employees (SEIU)	650,000
State, county, and municipal employees (AFSCME)	1,100,000
Steelworkers (USWA)	1,230,000
Teamsters (IBT)	2,000,000
Telecommunications workers (TIU)	50,000
Treasury employees (NTEU)	120,000
Typographers (ITU)	80,000
Utility workers (UWUA)	56,000

NOTE" Totals are rounded.

SOURCE WestIn, *Privacy and Quality of Worklife Issues In Employee Monitoring*, contractor report prepared for OTA, May 1986 Bureau of Labor Statistics, 1980, AFL-CIO estimates, supplementary inquiries at individual unions, 1984

[5] U. S. Congress, Office of Technology Assessment, *Automation of America Offices,* OTA-CIT-287 (Washington, DC: U.S. Government Printing Office, December 1985), p. 8.

[6] Ibid.

[7] During the course of this study, OTA spoke with a variety of union representatives having an interest in work monitoring, including the American Federation of Labor & Congress of Industrial Organizations (AFL-CIO), the Communications Workers of America (CWA), the Service Employees International Union (SE IU), Nine to Five: The National Association of Working Women (9 to 5), American Federation of State, County, and Municipal Employees (AFSCME), the American Federation of Government Employees (AFGE), and the Graphic Artists International Union (GAIU). In addition, 9 to 5 and AFGE were represented on this study's Advisory Panel. These unions, and many others, have taken a public stance against computer-based monitoring.

quality of work provided to the public. As an issue of job stress, unions see work monitoring-and particularly computer-based monitoring—as linked to *quality of worklife* issues, *worker solidarity, job design,* and *health* concerns. Worker *privacy* is also emphasized as a concern of the unions, particularly the rights of workers to see what records are being collected about their work performance.

Unions represent only a fraction of the estimated 4 to 6 million monitored employees, but from a field study of 110 business, government, and nonprofit organizations conducted for OTA, it is also possible to offer some observations on the attitudes of employees in general with respect to computer-based monitoring. The field study revealed that *fairness* in monitoring is a critical factor in clerical and customer service employee acceptance.[8] The emphasis on fairness highlights the fact that both *process* and *substance are* involved in how employees respond to electronic work monitoring. In addressing process, employees seek genuine involvement in the design, testing, application, and subsequent adjustment of new office systems technology. Substantively, the perceived reasonableness of monitoring depends on: 1) the fairness of the standards set, 2) the fairness of the measurement process employed, and 3) the fairness of the way measurements are used in employee evaluation. A breakdown of these key issues is given in table 12.

Table 12.—Key Issues and Problem Areas in Monitoring Clerical and Customer Service Workers

Key issues/problem aspects
1. **Fairness of work standards**
Do standards fairly reflect the average capacities of the particular work force?
Will they create unhealthy stress for many employees?
Do they account for recurring system difficulties and other workplace problems?
Do they include quality as well as quantity goals?
Do they represent "fair day's pay for fair day's work?
Do employees share in productivity gains achieved through new technology?
2. **Fairness of measurement** process
Do employees know and understand how the measurements are being done?
Can measurement system be defeated, impairing morale of those willing to follow the rules?
Do employees receive statistics on performance directly and in time to manage work rate?
Is relationship between quality and quantity communicated by supervisors when discussing problems with performance levels?
Do supervisors communicate clearly that they are taking system/workplace problems into account?
Are group rather than individual rates used when such an approach is more equitable?
Is there a formal complaint process for contesting the way work data is used?
3. **Fairness in applying measurements to evaluation**
Are there meaningful recognition programs for superior performance?
Is work quantity only one of a well-rounded and objective set of appraisal criteria?
Does employee get to see and participate in performance appraisal?
Is there an appeal process from supervisor's performance appraisal?
Is there a performance-planning system to identify and help performance problems?

SOURCE: Office of Technology Assessment, 1987

The computerization of communications refers to the fact that the information moving within modern communication systems, such as the telephone, is increasingly transmitted, routed, stored, and processed in digital form by electronic computers. Because of the computerization of communications, the use of employers' telephone systems can be tracked with greater precision and comprehensiveness than was possible previously. Computer software in some modern Private Branch Exchanges (PBXs), for example, permits station message detail recording (SMDR), a form of telephone call accounting that records from which telephone a call was made, what access code was used, where the call went, and how long it lasted. The call-accounting system can then generate detailed, comprehensive reports of all of the telecommunication activities of every employee in a firm.[9]

Telephone call accounting is an example of how the computerization of communications has placed work monitoring on the public policy agenda. A pilot study of unofficial use of

[8] Alan Westin, and The Educational Fund for Individual Rights, *Privacy and Quality of Work Life Issues in Employee Mom"toting,* contractor paper prepared for OTA, May 1986; field study conducted during 1982-84, and updated at all 110 sites during 1985-86.

[9] See ch. 3 for a more detailed discussion of telephone call-accounting systems.

Federal Government long-distance telephone usage has been completed,[10] and the implications of this study for employee privacy caused concern in both Congress and the press.[11] Although most of these concerns were over the manner and method by which this study would be carried out (and are therefore addressed below), at least some of the concerns are over the purposes for which it might be used. One concern, in particular, is that call accounting might be used to discourage whistleblowers, to stifle dissent or union activity, or to limit news media access to information.[12] Plans are being made to audit Federal employees' long-distance calls on a regular basis, raising additional concerns about the vigilance with which privacy concerns are addressed. The Office of Management and Budget (OMB) has issued proposed guidelines on compliance with the Privacy Act, in contemplation of a permanant call-accounting capability in executive agencies.[13] In the private sector, where about 30,000 call-accounting systems have been sold,[14] there are similar concerns over privacy and the potential for misuse. The issues surrounding the purposes of call accounting, in both the public and private sector, are considered in more detail below.

Finally, heightened public and worker expectations regarding privacy, health, and work-life quality help to explain why monitoring has emerged only recently as a public policy issue. The period from 1965 to 1986 saw the growth of concern over privacy in the public consciousness,[15] in the courts and legislatures,[16] and in the scholarly literature.[17] The concern over privacy during the past 20 years largely tracks the introduction and proliferation of the computer as a basic tool for the emerging information economy. It is no surprise, therefore, that privacy issues have made their way to the office environment, where computers have had their most pervasive influence. As we will see, however, the concept of privacy maybe inadequate to address most of the issues involved in work monitoring.

At the same time as privacy became an important theme in public policy, there were rising medical, media, and public concerns about the health effects of stress at the *office* workplace. Studies showed that stress among office workers was a contributing cause of ad-

[10]The unofficial use of the Federal Telecommunications System (FTS) or other government-provided long-distance services is illegal. 41 CFR 201-38.007 and 5 CFR 735.205. For a detailed discussion of the "Telephone Call Reduction Initiative," conducted by the President's Council on Integrity and Efficiency (PCIE), General Services Administration, and the Office of Management and Budget, see ch. 3.

[11]In March of 1985, Rep. Don Edwards (Chair, Subcommittee on Civil and Constitutional Rights) and Patricia Schroeder (Chair, Subcommittee on Service) sent letters questioning OMB Deputy Director, Joseph R. Wright, on the privacy problems involved with the study. The ACLU, The New York Times ("U.S. Phones Raise Issue of Privacy: New Equipment Would Provide Detailed Record of Calls," Burnham, Mar. 17, 1985), The Federal Times ("Planned Phone Audit Brings Blast From Several Groups," Montague, Mar. 25, 1985) and the Washington Post ("U.S. Agencies Use High Tech To Curb Workers," May 9, 1985) and considerable televisions coverage all brought public attention to the subject.

[12]Letter of Rep. Edwards to Joseph Wright, question No. 6. Mr. Wright's response was that the program would not be looking at local calls, and that long-distance calls to news media, congressional offices, public interest groups, etc., would be considered business calls for purposes of the study.

[13]Notice by the Office of Management and Budget, 51 Federal Register 18982 (Friday, May 23, 1986).

[14]See ch. 3.

[15]See *e.g., The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy,* conducted for Sentry Insurance by Louis Harris & Associates and Dr. Alan F. Westin, 1979. The survey revealed, among other things, that strong majorities of full-time employees believed that it was no longer proper for employers to ask job applicants about many topics that had once been traditional to collect (e.g., information on an applicant's spouse, neighborhood, membership in organizations, residential status, arrest, and similar matters). A 1983 Survey, also by Harris & Associates, reaffirmed the importance of privacy in the public mind.

[16]Over 20 Acts of Congress have been passed since 1970 to address problems of individual privacy. See: U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy,* OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June, 1986), p. 15. Most recent legislative efforts to protect privacy include the *Counterfeit Access Fraud and Abuse Act of 1985* and the *Electronic Communications Privacy Act of 1986.* None of these statutes are addressed specifically at employment, however. At the State level, 21 States have passed legislation dealing specifically with the confidentiality of employee records, and 34 States have statutes concerning the use of the polygraph in employment. *Compilation of State and Federal Privacy Laws (1984-85* cd.) (Washington, DC: Privacy Journal), and January 1986 supp.

[17]See, e.g., Robert Ellis Smith, *Workrights,* Westin, *Computers, Personal Administration, and Citizen Rights,* U.S. National Bureau of Standards Special Publication 500-50 (1979), and the report of the U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society (1977). See also:* OTA, *Electronic Record Systems,* op. cit.

verse health impacts, such as heart disease, and that *clerical* workers—because of their "high demand/low control' working situations —were among the occupations in office work most "at risk. "[18] Although the studies did not find harmful stress dependent on computer use (high levels of stress did show up in high-production, closely monitored clerical work that was not computer-based), the growing number of "machine paced" and "machine monitored' computer-based clerical workers generated similar concerns over stress and health.

The workplace context in which privacy and health concerns fermented was also changing. Women comprise roughly half of the work force in America today and are especially vulnerable to the impact of microelectronics on the work environment. [19] Accompanying shifts in the structure of American industry, from heavy industry to service and information sectors, was a growing recognition of workers' legal rights—quite apart from those obtained by collective bargaining.[20] These new rights are being introduced primarily at the State level, and include right-to-know, privacy, safety, and discrimination laws. What impact the increasing alarm over drug abuse and subsequent drug testing will have on this trend toward greater legal protection for workers is uncertain.

Of course, understanding the factors that have made monitoring into a public policy issue is of little help in understanding what the specific issues are, and why *electronic* monitoring raises problems that differ from conventional forms of work monitoring. Part II addresses these questions.

"of 130 common occupations, the following 12, ranked from most to least stressful were said to be most stressful:

1, Laborer	7. Manager/ administrator
2. Secretary	8. Waitress/waiter
3 Inspector	9. Machine operator
4 Clinical lab technician	10. Farm owner
5, Office manager	11, Miner
6. Foreman	12. Painter

(as reported in Meeks, "Worker's Compensation and Stress," 37 *CPCUJ* 171, 174-'75 (1984)[based on a 1977 NIOSH study]). See ch. 2 of this report, which discusses the NIOSH study in greater detail.

[19] See: Hartmann, Kraut, Tiny (eds.), (on] purer *Chips and Paper Clips: Technology and Women's Employment* (Washington, DC: National Academy Press, 1986).

[20] See, e.g., "Beyond Unions: A Revolution in Employee Rights is in the Making, " *Business Week*, July 8, 1985 (cover story); and "The New Industrial Relations, " *Business Week*, May 11, 1981; and more recently, *U.S. Labor Law and the Future of Labor-Management Cooperation*, BLMR 104 (Washington, DC: U.S. Department of Labor, Bureau of Labor-Man agement Relations and Cooperative Programs, 1986).

PART II: FRAMING THE DEBATE

As seen in the first section of this chapter and elsewhere in this report, electronic monitoring raises a variety of distinct concerns ranging from worker participation in job design, to worker solidarity, to privacy, to stress and health, to worker dignity, to quality of worklife, and more. Yet not all of these concerns are of the same type; some relate to the way that electronic monitoring is implemented in a given work environment, some to the use of monitoring to drive the worker, some to the use of information gained in monitoring, and some to the very fact that monitoring is conducted at all. Moreover, these concerns differ, depending on the type of monitoring being discussed; computer-based monitoring raises the issue of stress, while telephone call accounting engenders concerns over privacy. Clearly, electronic monitoring is a multifaceted issue, with no simple term of analysis.

Furthermore, upon close scrutiny, objections to electronic monitoring resist categorization in terms of traditional legal and normative principles. As the legal analysis in part III of this chapter shows:

- Except when monitoring is used for illegal ends, even some of its more onerous forms (e.g., machine pacing) are entirely legal.
- The concept of privacy, whether based on law or on ethical considerations, seems too narrow to address many concerns over the types of employee monitoring considered

in this report. The performance of tasks at work is, for the most part, an inherently public activity, which is done on behalf of the employer at the place of employment. An employee would likely find it difficult to assert a right of privacy in his or her performance at tasks such as computer claims processing.

- Although some legal doctrines may be implicitly-aimed at-vindicating a person's claim to bodily or mental integrity, autonomy, or dignity, the law recognizes no "right of dignity" or "right of autonomy' as such.[21]

Not only does monitoring escape the "net" of what is normally considered private information, its infusion into the workplace seems so gradual an extension of past practices that, if there is no real basis in doctrines of privacy for objecting to the proverbial supervisor with a clipboard, there *seems* to be none to using a computer to do much the same thing. As chapter 1 explained, some form of work monitoring has always been apart of employment, and the fact that technology introduces new or more efficient ways to monitor work may not be in itself an obvious incursion on privacy. Some reason must therefore be found why monitoring work by means of microelectronics is significantly different from past forms of monitoring, and what this difference means in terms useful for formulating policy.

Table 13.—A Framework for Addressing Electronic Work Monitoring

	Concern	Criteria
Purpose of monitoring	Fairness	Relevance Completeness Targeting
Manner and method of monitoring	Autonomy	Intensiveness
	Dignity	Intrusiveness
	Privacy	Visibility Type Leakiness Permanence
Effect of monitoring	Health	Frequency
	Stress	Continuousness Regularity Control

SOURCE: Office of Technology Assessment, 1987

To that end, OTA has developed an analytical framework that draws on familiar concepts and applies them to the new capabilities and characteristics of electronic monitoring. Table 13 summarizes this framework. In general, most claims about the deleterious effects of electronic monitoring can be understood as statements about *its purpose, its manner and method* of implementation, *or its effects.* It is this framework that guides the discussion in the rest of this chapter. In this part of the chapter, the purpose/method/effect breakdown is examined, in light of the characteristics of monitoring technologies, to show why electronic monitoring may present unique problems for the relationship between employee and employer. Then, in part III, the variety of legal mechanisms for addressing problems in the purpose, method, and effect of monitoring are examined. Finally, the chapter looks at the types of claims the law does *not* address, and explores the options Congress may wish to pursue in light of these unresolved issues.

[21] Consider, for example, the common law torts of:

(1) **Battery,** which is an intentional and unconsented-to contact, and in which "[t]he element of personal indignity has always been given considerable weight";

(2) Assault, which stems from an interest in freedom from apprehension of a harmful or offensive contact (as distinguished from contact). This individual is protected against a purely mental disturbance of his personal integrity, Damages are recoverable for mental disturbance (fright, humiliation, etc.) as well as any physical illness that flows from it, but an assault must create an apprehension of immediate physical harm; and

(3) Infliction of Mental Distress, an action in which the infliction of mental injury itself became vindictable. It is most often found in cases of intentional, flagrant acts, where "extreme outrage' of a defendant's act allows recovery ("your husband has been in an accident "–or situations in which there is repeated hounding or threatening of the plaintiff). Mental distress must exist and be severe, and no recovery can be obtained for mere profanity, obscenity or abuse.

W.L. Prosser, *Presser on Torts*, 4th ed. (St. Paul, MN: West Publishing Co., 1971), pp. 802 *et seq.*

Some court opinions suggest a close correlation between common law rights of privacy and individual dignity, autonomy, and personal freedom. For example, in Gerety, "Redefining Privacy, " 12 *Harvard Civil Rights and Civil Liberties Law Journal 233-296,* the author reviews several opinions dealing with the common law right of privacy, and concludes that:

> . . . [n]o fair measure of damages-general or specific-can be arrived at until we acknowledge that it was not the unexcused touching or the unwarranted search as such that caused the injury. What was injured, rather, was that peculiar aspect of dignity and freedom invested in reasonable expectations of privacy.

Id. at *265* (emphasis added). Although it may be the case that privacy rights entail interests in dignity and freedom, the converse does not necessarily follow: interests in dignity, freedom, and autonomy are not necessarily privacy interests. To vindicate interests in dignity and autonomy, in other words, requires a separate and independent basis in law, such as privacy.

Purpose

Concerns about the purpose of monitoring refer to the ends that the employer seeks to further through a given monitoring technique. By and large, electonic work monitoring may be used to measure and document a variety of employee transactions, for purposes of:

- planning and scheduling personnel and equipment;
- evaluating individual performance and personnel decisions (promotion, retraining, discharge, etc.);
- increasing productivity by increasing individual performance (feedback on speed, etc., and work pacing);
- providing security for employer property (including intellectual property) and personnel records;
- investigating incidents of misconduct or crime, or human error; and
- increasing management control, discouraging union organizing activities, identifying dissidents, etc.

Attacks on the purpose of a monitoring system can be understood as complaints about its *fairness.* While illegal monitoring purposes present little difficulty for finding the practice unfair (see part III), its use for currently legal purposes is more problematic. In general, employees and unions oppose the use of monitoring for purposes which, while legal, they regard as unfair. For example, electronic evaluations of employee performance that reflect inadequately or arbitrarily the task the employee is performing, or that place demands on workers' time and energy that are unrealistic or unduly burdensome, are likely to raise objections by employees and unions.

Because electronic monitoring represents an unprecedented ability to measure job performance exhaustively and in great detail (see chs. 2 and 3), several monitoring system characteristics become key items in ensuring fairness; particularly the *relevance, completeness,* and *targeting* of the monitoring.[22]

[22]These factors are illustrative of the types of concerns raised because of new technologies; they are hardly exhaustive, and the reader may have his or her own in mind.

Relevance.—A work monitoring technique that is relevant is one that measures performance related to the goal that the monitoring seeks to further. Thus, if billing customers in a timely fashion is the goal, a relevant measure would be whether customers were billed on time. A less relevant measure would be the number of "fields" in a customer account database that are filled in per hour.

Completeness.–A monitoring system is complete if it takes into account all, rather than some, of the performance parameters relevant to a given goal or behavior. If, therefore, a job entails both talking with as many customers as possible during a given time and handling customer needs in a satisfactory way, a monitoring system that measures only the number of customers handled is incomplete.

Targeting.-A monitoring system that generates information on particular individuals within an organization, rather than the group or work process of which that individual is a part, is a targeted system. A monitoring system that reveals only aggregate organizational performance is "untargeted" or categorical.

Using these definitions as measures of the fairness of monitoring technologies, one can begin to understand why new technology raises issues of fairness of purpose. For example, in computer-based monitoring, where a computer is used to tabulate total keystrokes during a given period of time, the question of the *relevance* and *completeness* of keystroke monitoring to the overall task can become a point of contention. In contrast to nontechnological methods of measuring keystrokes, such as a typing test (where typing speed may be relevant only to qualifying for a job), computer-based keystroke monitoring may make typing speed an end in itself, without regard to the purpose for which speed is valued-meeting a deadline as part of an overall project goal, for example. An overreliance on typing speed might also become an isolated, incomplete measure of job performance.

In telephone call accounting, issues of *completeness* and *targeting* become important to ensuring fairness. If, for example, the purpose of the audit is to reveal excessive numbers of long-distance calls, failure of the call-account-

ing system to also reveal extenuating circumstances may be deemed unfair. If the call-accounting audit targets specific individuals, rather than "cost centers, as abusers of long-distance service, failure to implement special procedures for giving notice to that individual, hearing explanations, and allowing challenges may give rise to charges of unfairness.

In service observation monitoring, fairness may require providing safeguards to subjective supervisory judgments about the operator's quality of customer service. In other words, if the purpose of the monitoring is to evaluate overall employee performance, it may be claimed unfair unless a more *complete* method of evaluation is used.

Many of the complaints reported to OTA about electronic monitoring suggested that *monitoring may itself change what counts as a relevant or complete measure ofjob performance.* If, for example, a job previously entailed finishing a given batch of insurance claims by the end of a week, a monitoring system that only measures the number of claims finished per hour may change that job by changing what counts as a relevant measure of performance, and by foreshortening the time in which a goal is to be achieved. The means for assessing performance may often become an end in itself.

Similarly, a monitoring system that is incomplete, or measures only one of several job parameters, may unintentionally change the nature of the job itself. If, for example, only quantity is measured, quality maybe sacrificed,

Manner and Method

Method refers to what information is gathered by monitoring, how it is gathered, and what is done with it once gathered. As such, issues about the manner and method of electronic monitoring reflect concerns about worker *autonomy, dignity,* and *privacy. Care* should be taken in reading these words in a too narrow or legalistic way—particularly the word privacy. As we shall see, few of the concerns electronic monitoring and privacy can be vindicated in a court of law. Nevertheless, complaints about a loss of autonomy in job decisionmaking, about the indignity of being "watched" by a machine, or the invasive feeling of having one's every move at work recorded, reflect deeply held societal values. In a work environment, we expect, and indeed hope, that our performance will be evaluated by our superiors, yet we may balk at the thought that someone will be constantly watching "over our shoulder. "

The reason why concerns about autonomy, dignity, and privacy are raised in electronic monitoring has to do with the fact that computers are ever-vigilant; unlike human supervisors, they do not tire of observing and recording the minutiae of employee performance. In some cases, computers are also being used to pace workers to speed their work rate.[23] In the process of using computers as surrogates for immediate human supervision, employees may complain of "dehumanization" and isolation. They may perceive themselves as a component of a system, rather than as human actors involved in and concerned with a larger enterprise. It is not difficult, under such circumstances, to understand complaints about a loss of autonomy and dignity:

> The electronic monitoring is one of the most offensive and pernicious aspects of our jobs. 1984 is nowhere more apparent than in the electronically monitored Equitable office. We "clock in" at 7 a.m. and from then until the end of the day, the VDT is counting every keystroke. At the end of the day, managers have a computer read-out from which productivity is determined and then averaged with subjective factors such as attitude to determine our rate of pay. Being watched, counted, and paced by a machine makes it very difficult to take pride in your work.[24]

It should be emphasized, however, that the potential for creating an onerous work environment through electronic work monitoring is not always realized. Indeed, whether computer-based work monitoring becomes "offen-

[23] See ch. 2.

[24] From Alan Westin, and The Educational Fund for Individual Rights, *Privacy and Quality of Work Life Issues in Employee Monitoring*, contract paper prepared for OTA, May 1986, p. 76; taken from testimony before House Subcommittee (?) 1984.

sive and pernicious depends crucially on *the manner and method* by which the system is administered, and what the overall work environment is like. For example, one of many interviews conducted for OTA, by Alan Westin, told of a suburban newspaper's circulation and classified ad department that monitored records via visual display terminal (VDT) in a way that minimized complaints:

> The management has a daily job chart that records each operator's time on and off the machine, errors made, and accounts handled. "I don't mind that at all, " Alice said. "They don't judge us on the numbers here; they take into account changes in the business service we are making, and the way customers—some of them–need more service than others. Its not a Big Brother thing. " She also noted that management's attitude led employees to cooperate informally to take heavy loads off one another when the calls piled up at one or two stations. Alice also said that the pay was "OK" by not "great" at this newspaper, but she liked the job very much because "the benefits are excellent, you can take courses at night and have the company pay for it, and people you work with are fun to be with. "

Several characteristics of electronic monitoring systems seem to be key to preserving worker autonomy, dignity, and privacy:

- Intrusiveness.— Intrusiveness is concerned with the degree to which monitoring involves probing the individual's body or mind. A monitoring technique that is intrusive is one that requires an individual to reveal facts about his or her thoughts, beliefs, or states of mind; to submit samples of body fluids or tissues, or to expose body parts not ordinarily exposed. A monitoring technique is *not* intrusive if the information collected thereby is obtained without probing into the person's mind or body. Note that intrusiveness concerns *how* information is gathered, and not *what* that information is.[25] Techniques may be intrusive even if the information they yield is information ordinarily observable.
- Intensiveness.– Intensiveness is the amount of detail about a worker's performance that monitoring reveals. An employee log of personal calls made on an employer's phone reveals only the number of personal calls. A telephone call-accounting system reveals much more detail; i.e., length of call, destination of call, the number called, which phone was used, time of day, etc.
- Visibility.-Visibilitv refers to the degree to which monitoring is apparent to the person being monitored. A computer-based monitoring system that reports back to the employee information on the number of keystrokes entered is more highly visible than one that reports this information only to supervisors. In general, the more visible the monitoring system, the more control the employee has in matching his or her performance to expectations. Visibility is important in part because of its influence on the psychology of power relationships at work. Whereas unaided monitoring by a supervisor may require a face-to-face confrontation with the employee—which both informs the employee that he or she is being monitored and 'humanizes' the monitoring by allowing explanations and personal interaction—electronic monitoring allows the supervisor to remove him or herself from the situation and use the machine as intermediary, thereby avoiding the human relationships that act as a corrective to overly rigid work environments.
- Type.—Type refers to the nature of the information gathered through monitoring. Information can be either *substantive* or *transactional.* Substantive information concerns the actual content or meaning of communications or documents. Transactional information is information about substantive information; the number or type of messages sent, to whom, how often, in what sequence, etc. Telephone service observation is an example of monitoring substantive information, since it

[25] For example, pumping the stomach of a person suspected of "possessing' illegal drugs is intrusive. See, e.g., *Rochin v. California*, 342 U.S. 165(1952) (The fourth amendment guarantees physical security of one's person against procedures that "shock the conscience.

reveals the content of employees' phone conversations. Telephone call accounting, by contrast, reveals only transactional information, such as the destination called, length of call, cost of call, etc. The distinction between substantive and transactional information can become blurred, especially where computers are used to piece together patterns of transactions, thus allowing inferences regarding the substantive content of those transactions. The distinction is important, since both societal expectations and the law generally endow substantive information with greater importance and protection.

- Leakiness. -Leakiness refers to the ability of information gathered by monitoring for one reason to be used for another. Thus, information gathered through telephone call-accounting systems tends to be leaky, because the information gathered can be used to track individuals' extra-work activity, despite the fact that it was collected for purposes of detecting abuse. Computer-based keystroke monitoring, on the other hand, tends to be relatively "tight," since the information gathered often has little use outside of the context of job performance. Like other criteria, leakiness is a factor in determining the legality of certain information practices.[26]
- Permanence. —Permanence refers to whether the information gathered by monitoring becomes a record, and how long that record remains in an employee file. Some information obtained by monitoring is transient, and never becomes a record. A computer-based monitoring system that determines when the employee has finished a certain job and is ready to move on to the next (i.e., machine pacing) may generate no records, and is thus transient. Telephone service observation, on the other hand, may entail writing comments on an evaluation sheet, which then becomes part of the employee's permanent record. Permanence is important from a privacy standpoint, since privacy law very often regulates what may be done with records that are permanent.[27]

The way in which these factors interact with electronic monitoring to give rise to problems of autonomy, privacy, and dignity can be illustrated by a brief consideration of the technologies considered in this report.

Computer-based monitoring may be implemented in an *intensive* and *invisible* manner. In other words, the computer can be used intensively to chart periods of peak performance at a VDT, time spent away from the terminal, time spent idle, and other minutiae of job performance. The monitoring may be of extremely low visibility-the employee may not know *how* she is doing, but does know *that* she is being "watched." The knowledge that one's every move is being watched, without an ability to watch the watcher, can create feelings that one's privacy is being invaded and that one is an object under close scrutiny. Being subject to close scrutiny without an ability to confront the observer may mean the loss of a feeling of autonomy. This may have subtle yet profound implications for interpersonal power relationships at work. In French philosopher Jean Paul Sartre's analysis of relationships between persons, he observes that:

> . . . [w]ith the Other's look the "situation" escapes me. To use an everyday expression which better expresses our thought, I am *no longer master of the situation .28*

Activities at work that cannot in fact be observed, measured, and thus controlled, are by default discretionary activities. In the past, the time an employee spent going to the bathroom, talking with his or her spouse, pausing between tasks, and so on, were largely discretionary. Obtaining detailed information on such activities was either impossible, impractical, or not cost-effective. What constituted "acceptable" employee performance was in

[26] See part III of this chapter.

[27] See the discussion of "system of records" under the Privacy Act in part III.

[28] Sartre, *Being and Nothingness*, as reprinted in The *Philosophy of Jean-Paul Sartre* (New York, NY: Vintage Books, 1972), p. 203. Emphasis in original.

part a function of the information a supervisor could collect. There was some domain of behavior which an employee could call his own, and for which he knew he was unaccountable.

But, because the computer dramatically enhances the intensiveness of human observation, the employee may feel powerless and exposed under the gaze of electronic monitoring. And, since face-to-face exchanges between employee and supervisor often involved negotiations and room for human error and "slippage" in the performance of tasks, the employee's relationship to a supervisor was on more even footing. But with systems of evaluation that are invisible to the employee, the transactions between people that allowed the employee to assert his autonomy may be minimized.

Different sorts of concerns about privacy and autonomy are present in telephone call accounting. Call accounting raises questions about the *permanence* and *leakiness* of records generated. The legal implications of these factors are dealt with below, but here we call attention to the effect of the existence of records on employee behavior. If records of all calls are being kept, the employee knows he or she may be required to justify those that are 'questionable. ' Under these circumstances, an employee may be less inclined to make calls that cannot be easily justified as business calls. This may have an impact on "whistleblowers - those seeking to disclose unethical or illegal corporate or government activity. Although reprisals against the whistleblowing employee may be forbidden by law or company policy, the knowledge that all of one's long-distance or even local calls are being accounted may nevertheless act to "chill" such activities. Even calls that can be justified as "business" or "official" may be subject to supervisors' judgments regarding propriety or business sense. And, although the employer does have a right to protect its property by ferreting out nonbusiness calls, the process of identifying the destination and identity of nonbusiness calls may compromise an employee's desire to conceal the identity of persons he or she is calling.

In short, automated telephone call accounting systems, if implemented in a pervasive fashion throughout government and business, may go "wide of the mark, " and have incidental impacts on employees' calling decisions, and perhaps on the employer-employee relationship, which were not anticipated. While in the past, employers had no choice but to treat employees as *if* they were honest,[29] the ability to store and process massive amounts of data may reverse this *de facto* presumption. Implicit in the installation of call-accounting systems is the proposition that at least some employees cannot be trusted in their use of the employer's property. While the proposition may in fact be correct, the system nevertheless audits the calling activity of *all* employees, treating each as a potential abuser of facilities. Moreover, as the ability to detect abuse is refined through technology, the standard of what constitutes an abuse may be lowered—while previous technology capabilities only allowed an employer to pay attention to extraordinary costs, new telephone call-accounting systems may allow assessments of calls that are "unnecessarily long" or "redundant."

Customer service observation shares many of the same characteristics with other monitoring systems. *Visibility* seems an important factor in assessing the manner and method in which customer service observation is carried out. The practice of listening in on employee telephone conversations with customers is not new, nor is it the result of recent technological innovations. It is also not essentially *electronic* monitoring, but instead a variant on human supervision and observation of employees. But, since today's technology permits a supervisor to listen in on an extension at a remote location with no audible "click' or diminution in volume, service observation is also a relatively low visibility form of monitoring. These factors have lead at least one organization, the Newspaper Guild, to complain that

> . . . the [employee's] inability to tell under the present equipment whether or not she is being monitored has inevitably given rise to feel-

[29] The basic tool for measuring abuse-the monthly telephone bill–was inefficient (requiring a human to scan and "flag" expensive calls) and revealed only flagrant abuses.

> ings of concern, nervousness and insecurity and has made the job. . . additionally and unnecessarily burdensome.[30]

In addition, telephone service differs from other forms of monitoring in that it reveals a substantive type of information; i.e., the content of employee conversations. As is discussed in part III of this chapter, privacy concerns are most often present where the type of information being gathered is substantive, rather than transactional. Because of this, courts have held that employers can only listen into business, and not personal, phone calls. Recognizing employers' needs to monitor the quality of service its representatives offer, no court has held service observation to be unlawful per se.

Effects

Unlike concerns over the purpose, manner, and method of monitoring, concerns over its effects are more tangible, less value laden, and are directed at the physical and psychological well-being of the employee. Because of this, most parties opposing monitoring have couched their arguments in terms of observable, objective effects on employee health caused by the stress involved in working at a monitored job. As we saw in chapter 2, however, proving that monitoring causes stress can be very difficult, and reliable data hard to find.

Electronic monitoring may create new demands on employee time, attention, and speed that give rise to concerns about stress. Among the factors that cause these concerns are the *frequency*, *continuousness*, *regularity*, and *control* involved in the monitoring. Each of these is described and discussed below.

- Frequency. — Frequency refers to how often the act of monitoring takes place. A call-accounting audit or computer-based keystroke monitoring that is conducted once **a year** is obviously less frequent than one that is conducted daily or weekly. Frequency is an important criterion because in combination with other criteria, such as *continuousness* and *regularity*, it may make the difference between monitoring as sporadic "spot checks" for efficiency and monitoring as a part of the daily job environment.
- Continuousness.–Continuousness is a measure of how constant a monitoring technique is. It is closely related to *frequency* and *regularity*, but refers to the duration of and intervals between monitoring. For example, a computer-based monitoring system that records every transaction, including time spent away from the keyboard, during an 8-hour workday would be highly continuous. A similar system that recorded only when the employee logged on and logged off would be relatively noncontinuous.
- Regularity. —Regularity refers to the predictability of intervals between monitoring. Thus, a telephone call-accounting audit conducted every month is highly regular; a random audit is not. Regularity is an important criterion, because it affects such issues as actual or constructive knowledge of being monitored, and it may play a factor in chronic stress (if monitoring is highly irregular, the employee may have to stay constantly "on guard" to the possibility of monitoring).
- Control.–Control refers to the ability of the employee to set his or her own pace of work, and to use discretion in organizing and executing a task. An employee who can determine the pace at which discrete tasks, such as filling out claim forms, are completed has relatively greater control than one who doesn't.

Electronic monitoring may involve changes in each of these factors, and may therefore cause greater stress than other forms of observing or measuring employee performance. In computer-based monitoring, for example, an employee's *control* over the pace of work may be given over to the machine; when one claim form is filled out, another pops up on the

[30] ('From proceedings of an arbitration of a grievance filed by the Newspaper Guild against the Boston *Herald Traveler, Boston Herald Traveler Corp.,* Case No. 1130-0291-68, arb. award, Nov. 12, 1969; as cited in Alan Westin, and The Educational Fund for Individual Rights, *Privacy and Quality of Work Life Issues in Employee Monitoring,* contractor paper prepared for OTA, May 1986, p. A-16.

screen, and delays in processing the second are being recorded. The machine sets the pace. This may conceivably cause stress. On the other hand, in customer service observation, *continuousness* and *regularity* may be the factors causing stress. Whether these, or any other, characteristics of electronic monitoring factors do in fact cause stress is the subject of some debate, as will be discussed in part III.

Where Is the Future of Monitoring Headed?

The full extent of electronic monitoring techniques may have yet to be realized, and we might see monitoring expand into more and different jobs. The only limit, in principle, is the technology itself. Advances in technology may allow a greater range of less routinized tasks to be monitored. Sophisticated software design, called expert systems, in combination with the computerization of most office activity, may enable tracking the complex transactions of bank loan officers, sales and management personnel, and stock brokers. Profit center accounting software, for example, can keep accurate and timely information on such items as expense account and investment activity, interdepartmental funds transfer, and business expense structure and account turnover. Since many expert systems are applied to assist physicians in diagnosing disease, it is conceivable that such systems could also be used to monitor diagnosis and method of treatment decisions. Depending on the reliability record of these expert systems, and their acceptance in the medical community, compliance with expert systems' "decisions" may become *prima facie* evidence of a standard of due care for purposes of determining liability for negligence.

Advances in technology could change monitoring in the following ways:

- More types of information, including information about employees' behavior out of work, may become increasingly available.
- A greater amount of information about employee performance is now available through the use of technology. Sophisticated use of the computer to edit and digest this information allows it to be put to practical use.
- In general, the means for obtaining information about the individual are less physically intrusive than would be possible without technological methods.
- The storage capacities of modern information systems permits more information about employees to be retained as records. The growing use of computer networks also permits employee records to be distributed and shared more easily than paper folders.

Table 14.—Factors Affecting Electronic Monitoring

Factors favoring increased monitoring:
- Economics and increasing sophistication of the technology
- Labor market trends
- Macroeconomic trends
- Employer liability
- Vendor bandwagons
- Technological imperatives

Factors limiting increased monitoring:
- Employee backlash, morale, & turnover
- Diminishing returns
- Job deskilling or upgrading
- Information overload
- Management priorities

SOURCE: Office of Technology Assessment 1987

Technology is not, as a practical matter, the only limit on electronic monitoring. A variety of factors, aside from legislation, may influence the way in which monitoring technology is eventually used. The factors can be grouped into those that tend to favor an increasing amount of monitoring, and those that tend to limit monitoring. They are discussed below and summarized in table 14.

Factors Favoring Increased Monitoring

Because purchasing, maintaining, and using an electronic work monitoring system often involves considerable expense, monitoring is unlikely to be done gratuitously. Beyond achieving the stated goals of enhancing productivity or quality, or detecting and combating waste, fraud, and abuse, several factors in combination suggest that work monitoring may increase, both in terms of the sheer volume of businesses that monitor and the variety of monitoring techniques and work environments. Some of these factors include:

- The economics and increasing sophistication of the technology.—In the past, the economics of monitoring tended to work against intensive mass surveillance; paid employees were required to observe other employees. Modern monitoring techniques alleviate this fixed cost, labor-intensive approach, and substitute an approach with a near-zero marginal cost, which is capital-intensive. Monitoring systems may become cheaper to maintain than the cost of abuse or inefficiency in the labor force. And, although it is easy to overstate the importance of new technologies,[31] the permeation of microelectronics into most office technology means that monitoring can be fully integrated into work processes without the need for elaborate and costly independent measurement devices. Computer terminals and PBXs, for example, can be monitored through relatively simple and inexpensive changes in software.[32]

- Labor Market Trends.—Organized labor's share of the work force is currently between 18 and 19 percent of the nonagricultural labor force in America (down from a high of 35.5 percent in 1945), and it is expected to decline further over the next 15 years.[33] There is a concomitant shift in jobs from the manufacturing to service sector; precisely the sector in which monitoring is highest and unionization weakest. It does not necessarily follow from this that employee rights are being diluted,[34] but it may divert the source of employee rights from the provisions of labor-management contracts to statutory or common law; areas which, as we have seen, provide a paucity of protection against monitoring.
- Macroeconomic Trends.—Increasingly competitive international markets in the private sector, and decreasing agency budgets in the public sector, force employers to trim expenses, including those associated with labor. Monitoring is one way of accomplishing this.[35] At the same time economic insecurity within the labor market over finding and keeping a job tend to blunt the incentive of employees to "rock the boat, " particularly if it would entail lawsuits against employers.
- Employer Liability.—For a variety of reasons, it is the employer that generally suffers economic losses from the wrongdoings of its employees. Product liability, negligence, trade secret, and even criminal laws often ensure this result. Furthermore, plaintiffs in civil suits often look to the employer's "deep pocket, " rather than to just the employee, for redress. Jury awards may be very high. Under these circumstances, it is not merely prudent, but in fact mandatory, that the employer exercise a degree of oversight and control over its employees. Electronic monitoring may often be the least expensive and most thorough way of facilitating this.[36]
- Vendor Bandwagons.—Vendors of computer-based monitoring and telephone call-accounting software have an obvious interest in promoting their products. While some vendors are sensitive to privacy and

[31] For example, keystroke counters, called "cyclometers," were available for typewriters in 1913, and Taylorism developed a variety of sophisticated techniques for measuring output, sampling piecework, and counting units of production, See, e.g., Lee Galloway, *Office Management: Its Principles and Practice (New* York, NY: Ronald Press, 1919); and William Schulze, *The American Office: Its Organization, Management, and Records* (London: Key Publishing, 1913).

[32] The Integrated Services Digital Network (ISDN) may do much to accelerate this trend toward integration, since all transactional information can be reduced to commensurate, digital form. The first critical steps toward ISDN have already been taken, and will give users access to a broad range of communications and data processing services. See: Robert Rosenberg, "The Digital Phone Net Finally Starts Taking Off, " *Electronics,* Aug. 21, 1986, pp. 57-61,

[33] " Beyond Unions, " Business *Week*, July 8, 1985, pp. 72-77.

[34] Some think that the case is just the contrary: "Some business leaders think they will get a union-free environment, but what they may get is a legalized environment, according to Harvard labor law specialist, Paul Weiler, as quoted in *Business Week,* July 8, 1985, p. 73.

[35] A press release by OMB in support of its Telephone Call Reduction Initiative said, for example, that "the PCIE and GSA/OMB initiatives will address the reduction of the Government's long distance phone costs. "

[36] For example, by using a computer to track the accuracy of records maintained by employees to avoid liability for warranty or negligence in providing information; by sampling the communications and memos that go out of the office; or by using cameras to observe employee conduct.

other concerns, some tend to "puff" the savings that their systems offer.

- Technological Imperatives.—Monitoring measures many things that employers have always wanted to know. In addition, a manager is concerned with doing all that he or she canto increase efficiency and cut waste. Nor should one rule out an irrational, but common response to new technology: "if it can be done, it should be done. " Because of this, the use of monitoring technologies may become an imperative or an accepted way of doing business.

Factors Limiting Increased Monitoring

Not all factors indicate a headlong drift toward more widespread and intensive monitoring. Indeed, many factors seem to suggest that monitoring, if taken to extremes, may actually impede some of the goals that it seeks to further (e.g., productivity). Such factors may include:

- Employee Backlash, Morale, and Turnover.–Past attempts to drive employees to ever-higher levels of production through close supervision, surveillance, abuse, and threats of discharge have met with great resistance among workers.[37] Employee sabotage and informal collusive "slowdowns, " which tended to reduce production below the average, were often the result, even in nonunionized industries. During times of economic expansion, job turnover also increased. To the degree that automation is contributing to job upgrading (see below), turnover may become an increasingly expensive proposition, because of the time and money involved in training new employees.
- Diminishing Returns.-A monitoring system that emphasizes speed or volume, as many computer-based monitoring systems do, may often do so at the price of quality or accuracy. A computer-based monitoring system that counts keystrokes, for example, may engender a greater number of unintentional or intentional errors (e.g., holding one key to increase total number). According to a recent work on the subject, greater gains in productivity are often the result of a reorganized workflow and the integration of previously fragmented tasks.[38]
- Job Deskilling or Upgrading. -It is unclear whether office automation is stripping relatively skilled jobs of their discretionary and autonomous content (deskilling), or whether it in fact is taking the drudgery out of work, leaving the employee with a greater latitude for individual creativity (upgrading). Some studies have suggested that both deskilling and upgrading are occurring, sometimes within the same occupation.[39] To the degree that jobs are being upgraded by automation, work monitoring systems that require jobs to be routinized, and reducible to standardized units of production, may become less and less apropos of highly complex, nonstandardized work environments.[40]
  Information Overload.–Although electronic monitoring offers gains in efficiency over human observation, it very often requires that a human digest the information generated by the system and make managerial decisions based on that information. This in itself may require considerable investments of time and wages. The records generated by telephone call accounting systems, for example, can be quite voluminous, and often require a cadre of auditors to verify and interpret the results.[41]

[37] See: A. Gouldner, *Patterns of Industrial Bureaucracy* (Glencoe, IL: Free Press, 1954).

[38] Paul Strassman, *Information Payoff* (New York, NY: Free Press, 1985).

[39] P Attewell and J. Rule, "Computing and Organizations: What We Know and What We Don 't Know, *Communications of the ACM*, December 1984, vol. 27, No. 12, pp. 1184-1192; R. Kling and W. Sacchi, "Computing as Social Action: The Social Dynamics of Computing in Complex Organizations, *Advances in Computers*, vol. 19, 1980.

[40] Paul Strassman, *Information Payoff (New* York, NY: Free Press, 1985).

"See ch. 3 for an example of an expense report generated by telephone call accounting.

[42] R. Edwards, "Individual Traits and Organizational Incentives: What Makes a 'Good' Worker, " *Journal of Human Resources*, winter 1976.

- Management Priorities.—The kinds of information provided by electronic monitoring may not assist management in addressing the workplace inefficiencies that it perceives as most troublesome, and monitoring may frustrate the human relations goals that many firms see as a key to productivity. Among management's more pressing concerns are employee fraud and chronic absenteeism and tardiness;[42] conduct that requires no electronic monitoring to detector deter. Moreover, management may have no interest in monitoring systems that degrade worker responsibility and morale, since commitment to the job is perceived as a vital element of employee productivity .43

Wild Cards: Automation and Artificial Intelligence

It is possible that present concerns overwork monitoring may be rendered obsolete by machines whose functions are to substitute for precisely the type of job that is today the focus of monitoring. As mentioned in chapter 2, electronic monitoring is most often used in jobs that require relatively few skills, that are highly routinized, and that have more or less uniform patterns of input and output. This type of labor is gradually being substituted by automation. Data-entry work (whether numeric or textual in nature), for example, can be eliminated by:

- interorganizational transfer of data, directly from computer to computer;
- direct input of data by optical scanning technologies, and possibly by speech recognition technology; and
- capture of data at the point of origin, in a variety of ways ranging from bar code readers to consumer use of terminals, e.g., bank automated teller machines (ATMs).[44]

In conjunction with progress in natural language processing and pattern recognition systems,[45] this trend toward automation of highly routine jobs may end up eliminating narrow, low-skill clerical positions altogether, replacing them with multi-activity skilled positions." Highly complex jobs, requiring multifaceted decisionmaking, interpersonal skills, and "common sense" judgment, are unlikely to be as susceptible to electronic monitoring, since these jobs are not amenable to merely quantitative measures of performance.[47] Thus, it is possible that the issue of electronic work monitoring is merely a transient phase in the automation of office work. There are some indications, however, that data entry requirements are accelerating faster than the ability to automate them. So it may be quite some time before monitored jobs are automated out of existence.

[43]R. Walton, "From Control to Commitment in the Workplace," *Harvard Business Review*, vol. 35, No. 2, 1985, pp. 76-84; and "The New Industrial Relations," *Business Week*, May 11, 1981. See also: *Business Week*, "The Hollow Corporation" special issue, Mar. 3, 1986; *Business Week*, "High Tech to the Rescue," June 16, 1986; National Academy of Science, *Towards a New Era in the U.S. Manufacturing* (Washington, DC: 1986); and *Human Resources Practices for Implementing Advanced Manufacturing Technology* (Washington, DC: 1986).

[44]From U.S. Congress, Office of Technology Assessment, *Automation of America Offices, OTA-C IT-287* (Washington, DC: U.S. Government Printing Office, December 1985), p. 47.

[45]U.S. Congress, Office of Technology Assessment, *Information Technology R&D: Critical Trends and Issues*, OTA-CIT-268 (Washington, DC: U.S. Government Printing Office, February 1985), see especially ch. 3, "Selected Case Studies (Artificial Intelligence).

[46]U.S. Congress, Office of Technology Assessment, *Automation of America Offices, OTA-CIT-287*, p. 51. Of course, the low-skilled employee may be eliminated entirely. The consequences of automation for the job market are highly controversial, but it is unimportant for present purposes to enter the debate.

[47]This statement should be qualified by two caveats: any job performance can in theory be subjected to quantifiable, electronically monitorable criteria; and electronic monitoring of the future may be able to build in some sort of assessment of the qualitative features of job performance.

PART 111: AN OVERVIEW OF APPLICABLE LAW

The Framework for the Legal Analysis

Part II suggested that concerns over the purpose of monitoring can be understood as objections based on notions of fairness; that the manner and method in which monitoring is implemented may involve issues of dignity, autonomy, and privacy; and that issues involving the effects of monitoring can be largely understood as concerns over health and stress. The following legal analysis uses this framework by applying more specific legal concepts to the purpose/manner and method/effect framework, Table 15 shows the relationship of this framework to applicable law.

Each of the major types of monitoring considered in this report—computer-based monitoring, telephone service observation, and telephone call accounting–will, to the extent that they raise unique legal issues, be discussed separately. Otherwise, the analysis that follows is cumulative; what is said of computer-based monitoring, for example, applies equally to telephone customer service observation and telephone call accounting, unless specifically mentioned in the text.

Before proceeding with the analysis, it is necessary to discuss two issues common to all three types of work monitoring: the concept of employment-at-will and the differing legal status of private and public sector employees.

The Concept of Employment-at-will

Under the common law tradition in the United States, the relationship between employer and employee has been one of "employmerit-at-will. " Employment-at-will simply means that, in the absence of a specific agreement to the contrary, an employer has an absolute right to discharge an employee for any reason, and the employee has a correlative right to resign for any reason.'" Although subject to considerable erosion through a variety of judicial and statutory exceptions and qualifications (discussed below where relevant), [48] the employment-at-will doctrine is still law in all 50 States.

[48] S. Williston, Contracts § 1017 (1967); see e.g., *Pearson v. Youngstown Sheet & Tube Co., 332* F.2d 439 (7th Cir.), *cert de*nied, 379 U.S.914 (1964).The terminability y at will doctrine can be modified by a contractual agreement to retain the employee for a specified period of time require that the discharge of an employeee be based on a breach of that employee's obligations under the terms of his or her contract of employment.

[49] The claim of wrongful discharge, for example. has been accepted in a majority of States. ' 'To date, the common law of three-fifths of the states has recognized, albeit to markedly varying extents, a cause of action for wrongful discharge in one form or another. " Kenneth T. Lopatkay, "The Emerging Law of Wrong Discharge-A Quadrennial Assessment of the Labor Law Issue of the 80's, " 40 *Business Law 445 (1984),* and see: William L. Mauk, "Wrongful Discharge: The Erosion of 100 Years of Employer Privilege, " 21 *Idaho Law Review* 201 (1985).

Table 15.—A Framework for Addressing Electronic Work Monitoring

	Concern	Criteria	Example of applicable law
Purpose of monitoring . ., ...	Fairness	Relevance Completeness Targeting	National Labor Relations Act: Civil Rights Act; Merit System Principles (as administered in EEO, OS HA, ERISA, EPA, etc. [a]); State Law on Privacy; Constitutional Law[a]
Manner and method of monitoring . . .	Autonomy Dignity Privacy	Intensiveness Intrusiveness Visibility Type Leakiness Permanence	State Law on Wrongful Discharge: State Law on Privacy; PCIE Guidelines; Title III of Omnibus Crime Control and Safe Streets Act; Electronic Communications Privacy Act; National Labor Relations Act, Privacy Act of 1 974[a]
Effect of monitoring	Health Stress	Frequency Continuousness Regularity Control	Worker's Compensation Statutes on Stress-Causing Labor

[a] Applies only to Federal employees

SOURCE Of ficeof Technology Assessment, 1987

The significance of the doctrine of employment-at-will for electronic work monitoring lies in its practical effect on the legal or economic pressure that an individual employee can bring to bear against the employer. Unless the contract of employment includes either substantive prohibitions, such as work environment clauses that can be construed to extend to work monitoring, or procedural requirements, such as binding arbitration agreements, an employee who objects to being monitored has the options of accepting the practice, protesting the practice to the employer and facing possible dismissal, or leaving the job voluntarily. This is particularly true of Federal employees, who, though they are represented by the American Federation of Government Employees (AFGE), are forbidden by law to negotiate performance standards which are at the heart of many disputes over electronic monitoring.[50]

The Legal Status of Public v. Private Sector Employees

The legal rights of an employee with respect to electronic monitoring depend critically on whether the employer is a privately owned and operated firm or an agency or subdivision of the local, State, or Federal Government. As a general rule, an employee has no constitutional rights against private individuals, including private employers.[51] Therefore, even if some forms of monitoring can be said to infringe a constitutionally protected interest, that interest can only be vindicated if the employer is a local, State, or Federal Government, or if the employer is acting pursuant to or under authority of a statute or ordinance.[52] Furthermore, the Privacy Act of 1974, which may be relevant insofar as electronic monitoring often generates a system of records, applies only to records kept by the Federal Government. It is therefore significant primarily to Federal Government employees.[53]

Notwithstanding this crucial distinction between private and public sector employers, there are a number of State and Federal statutes that may be relevant to considerations of the purpose, the manner and method, and the effect of monitoring by *both* private and public sector employers. The public/private distinction is therefore considered below only where relevant.

Purpose

Computer-Based Monitoring

Computer-based monitoring is the computerized collection, storage, analysis, and reporting of information about certain employee work activities. Within this broad definition, the chapter focuses on the use of computer-based monitoring to obtain data about employees directly through their productive use of computer and telecommunications equipment. In all cases documented by OTA, computer-based monitoring is used by both public and private sector employers for entirely legal purposes. As a rule, an employer is not liable for endeavoring to further its legitimate business interests, such as enhancing productivity and

[50] 5 U.S.C. §43, The Federal Labor Relations Statute.

[51] This concept is known as "State action." It is a basic Principle of constitutional law, and provides that the rights secured to individuals by the 14th Amendment to the Constitution proscribe only certain actions by the state, state agencies or subdivisions, or individuals acting under color of State law, and do not limit actions between private individuals or private entities. See e.g., *Flagg Bros., Inc. v. Brooks, 436* U.S. 149 (1978). There are certain narrow exceptions to this rule, as where a company assumes all the functions of a municipality, *Marsh v. Alabama, 326* U.S. 501 (1946), or where there is substantial State involvement with a private entity, e.g., *Burton v. Wilmington Parking Authority, 365* U.S. 715 (1961). Some have argued that the actions of large private organizations that wield great economic power over individuals should be considered State action. See, e.g., Berle, "Constitutional Limitations on Corporate Activity-Protection of Personal Rights Invasion Through Economic Power," 100 *University of Pennsylvania Law Review* 933 (1952).

[52] Even in the latter case, the breadth of State action may in fact be very narrow. See, e.g., *Moose Lodge v. Irvis, 407* U.S. 163 (1972) (State liquor license for segregated dining room was insufficient State involvement).

[53] A provision that would have made the Privacy Act, 2 U.S.C. §552a (1976), applicable to the private sector was present in the original Senate version of the Act, S 3418, 93d Cong., 2d sess. $201(a), but was not adopted. The Privacy Act is, however, applicable to government contractors. 5 U.S.C. §552a(m).

quality. Nor is an employer liable for protecting its property, or for investigating misconduct or crime.[54]

Computer-based monitoring for purposes of advancing or protecting commercial interests and overseeing actions of employees is not merely prudent business practice—it may be a positive legal requirement.[55] In many instances, an employer is held vicariously liable for the torts or crimes of its employees, based in part on the theory that it is in control of and responsible for many of the actions of its employees while in the scope of their employment.[56] Furthermore, an employer, as a seller or even gratuitous supplier, may be liable for the quality of the goods, services, and perhaps even the information produced by its employees.[57] And, monitoring the flow of trade secret information out of a business concern may be necessary if an employer is to preserve its rights under trade secrets law.[58]

When used for certain purposes, however, computer-based monitoring may become the instrument of illegal ends. It is conceivable, for instance, that monitoring could be used to frustrate the rights of employees to organize, by being used as "punishment" for individuals seeking to organize.[59] OTA found no evidence that monitoring is actually being used in this way.[60]

It is also conceivable that monitoring might be used to discriminate against a class of employees, by placing stricter scrutiny and standards of job performance on certain groups. As mentioned in chapter 2, the highly specific information that monitoring generates often requires a considerable amount of interpretation, leaving great leeway for (intentional or unintentional) misinterpretation in the guise of "objective, " quantitative evidence. OTA found no case where monitoring was intentionally used for this purpose, but that does not preclude such a possibility.[61] It is important to point out, however, that the vast majority of employees whose work is monitored by computer are

---

[54] Based on one survey of the top three reasons for auditing the use of intelligent desktop terminals were:

- To prevent abuse of company PC resources for personal purposes.
- To prevent confidentiality/security breaches.
- To prevent violation of legal/regulatory duties in the use of client or employee data.

From Alan Westin, and The Educational Fund for Individual Rights, *Privacy and Quality of Work Life Issues in Employee Monitoring*, contractor paper prepared for OTA, May 1986.

[55] For example, a representative of American Express Corp., Inc., informed OTA that American Express is required by the Fair Credit Reporting Act to stop dunning a card member who writes in to say that he or she is having a dispute with a service establishment. Because the letters are computer generated, the only way that American Express can know it is in compliance is through its monitoring system, which aggregates all such transactions and reports on when they are made.

[56] See, e.g., *Prosser on Torts*, §69 (1971).

[57] The Uniform Commercial Code, adopted in 49 States, imposes on the seller of goods three different kinds of warranties. U.C.C. 2-313-315 Providers of services, such as insurers, may be liable for breach of either express or implied conditions of the contract. Information providers, such as database companies and weather forecasters, may be liable on several theories, such as strict liability, negligence, warranty, or defamation. See: e.g., *Aetna Casualty & Surety Co. v. Jeppesen & Co., 767* F.2d 1288 (9the Cir. 1985); and *Dunn & Bradstreet v. Greenmoss Builders, Inc., 105* S. Ct. 2939 (1985).

[58] A trade secret is a form of intellectual property that covers any confidential formula, pattern, device, or compilation of information used in a business, which gives that business an opportunity to obtain an advantage over competitors who do not know or use the secret. One of the factors for determining whether a business' secret is a trade secret is "the extent of measures taken by (it) to guard the secrecy of the information." *Restatement of Torts,* §757, comment B.

[59] Such rights are protected, for example, by the National 'a" bor Relations Act, 29 U.S.C. §151 et seq., which secures to employees "the right to self-organization, to form, join, or assist labor organizations . . ." Id., at §157. The use of monitoring to impose changes in working conditions-e. g., by accelerating machine pacing—may be illegal if done for the purpose of reprisal against employee organizational activity. 29 U.S.C. $158 (a) (3); See, e.g., *N. L.R.B. v. Sanitary Bag and Burlap Co., 406* F.2d 750 (3rd Cir. 1969) It is also possible that PC use could be monitored to detect union communications by searching or auditing PC-user disks or files, although there is no indication that this activity is widespread today. Monitoring for this purpose, however, would probably *not* violate labor laws, since employers may observe the activities of employees on its property during working time. *Stone & Webster Engineering Corp. v. N. L. R. B., 536* F.2d 461 (1st Cir. 1976); *N. L.R.B. v. R.C. Mahon Co., 269* F.2d 44 (6the Cir. 1959).

[60] One source told OTA that one practice in monitoring computer files is to check for human error. Under this circumstance, some privacy questions may raised, despite the legitimate purposes of the monitoring.

[61] For example, the veracity of computer monitoring records was the subject of an arbitration dispute between The State of Oregon Employment Division and the Oregon State Public Employees Union (affiliated with the SEIU), on behalf of one of its members. The employee was fired from her job as word processing specialist for allegedly tampering with her and others' production statistics generated by a Wang "Machine Statistics System. " The arbitrator found the statistics generated by the computer system reliable, albeit circumstantial, evidence that the employee had tampered with the system, and let the State's decision to terminate the employee stand. The union

(footnote continued on next page)

female, raising questions about the existence of de facto discrimination in working conditions.[62]

Finally, monitoring could be used as a method of detecting, preventing or retaliating against whistleblowers. This might be accomplished by restricting access to certain computer files for the purpose of preventing damaging information from being revealed, by tracking the types of files accessed by certain employees in order to ascertain the source of "leaks," or by imposing more onerous demands on certain employees for revealing evidence of waste, fraud, or abuse.[63] OTA again found no evidence that monitoring is being used for such purposes.

The number of illicit purposes to which monitoring can be put is limited only by the imagination, yet monitoring seems no more or less likely to lend itself to illegal retaliation than any other form of office technology (the paper copier or punch clock, for instance). However, the employee may often know that his or her computer files or phone calls are being "observed" by the monitoring system, and this knowledge may in itself act as a "chilling" device to would-be whistleblowers or union organizers. In a case example submitted to OTA by the AFL-CIO, the chilling effect of video observation was noted:

> . . . employer installed and focused TV monitoring equipment inside the plant on every work station and worker after organizing effort began. Monitors were not available for all to see, but viewed only by management in management office. Employer said monitoring was for safety reasons and would lower Worker Compensation insurance rates. In fact, no one could determine how that could be. During the height of organizing, two workers who left their work stations to go to restroom were suspended for leaving their work station, without permission. Monitoring had chilling effect on workers attempting to organize for purposes of collective bargaining, Of the 100 workers in the unit, 89 signed authorization cards calling for a recognition election. But when the final vote came, the union was 12 votes shy of a majority. . ."There was an unspoken fear that Big Brother would catch them talking for or working for that union.[64]

Even if the truth of this use of monitoring for alleged purposes of union-busting are not

(footnote continued from previous page)

disputes the arbitrator's findings, and suggests that the employee's "work station was frequently used by other employees, particularly her supervisor with whom she had a bad working relationship. From a "case study" submitted to OTA by the Service Employees International Union, and Westin, "Privacy and Quality-of-Worklife Issues in Employee Monitoring, " OTA Contract Report, December 1986. See also, *The Wall Street Journal,* June 6, 1985. The union thus suggests the possibility that the employee could have been "framed. Regardless of whether the employee in this case was in fact culpable for the alleged tampering, it is clear that monitoring systems are capable of being used for discriminatory or retaliatory reasons: the objective, mechanically produced measurements of productivity can be "rigged," and undue trust can be placed in machine printouts.

[62]See Title VII, Civil Rights Act of 1964, 42 U.S.C. 2000c (a)(l). The de facto feminization of monitoring may give rise to suits under the Civil Rights Act, since intent to discriminate is not a prerequisite to an action under Title VII.

[63]Federal employees have been protected by statute against reprisal for disclosing waste, fraud, or abuse in the Federal Government since 1979. As part of "merit system principles, " all employees of the executive branch of government, the Administrative Office of the U.S. Courts, and the Government Printing Office:

> . . . should be protected against reprisal for the lawful disclosure of information which the employees reasonably believe evidences—
> (A) a violation of any law, rule, or regulation, or
> (B I mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety
> 5 U.S.C. $2301(b)(9)

Additional protection may be available under anti-reprisal clauses of various substantive employee protection or public protection laws, such as EEO, OSHA, ERISA, EPA, and so on. Other public employees are protected under First Amendment principles, as articulated in *Pickering v. Board of Education, 391* U.S. 563 (1968) ("the interests of the [employee], as a citizen, in commenting upon matters of public concern [are to be weighed against] the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees. " Id. at 568. See also: *Mt. Healthy City School District Board of Education v. Doyle, 429* U.S. 274 (1977) (protected whistleblowing must be 'a matter of public concern" and play a "substantial part" in decision to fire); and *Connick v. Myers, 451* U.S. 138 (1983) (whether dissent is a matter of public concern is determined by content, form, and context of communication). In addition, 21 States have enacted whistleblowing statutes. "Beyond Unions, " *Business Week,* July 8, 1985, p. 73.
Employees in the private sector maybe protected under exceptions to the employment-at-will doctrine. See footnote 49.

[64]From AFL-CIO Case Examples, submitted to OTA. The technology allegedly used to monitor these employers was the video camera—a technology not considered in this report. However, software for computer-based work monitoring could be used to accomplish much the same purpose as alleged in this case study, by recording the time away from a station, by monitoring internal electronic mail and employee-generated documents, or by determining who was logged onto a particular work station.

born out, it nevertheless illustrates the heightened potential of monitoring used to deter the efforts of whistleblowers or union organizers. This potential is also explored below in the context of telephone call accounting.

Telephone Service Observation

Telephone service observation was described in chapter 3. It refers to the act of systematically intercepting the content of employee telephone calls by listening in on them. This is often done by a supervisor or quality control specialist to evaluate courtesy, accuracy, or compliance with company guidelines. It is a common practice in a host of businesses which sell products or service customers over the telephone. As mentioned in chapter 2, service observation is becoming integrated with various forms of computer-based monitoring, the legal implications of which were considered above. This section will consider service observation in isolation from other monitoring techniques.

The use of service observation for illicit purposes—e.g., to discourage or listen in on employee organizational activities, to discriminate against certain classes of employees, or to detect and punish whistleblowers—is subject to much the same legal analysis as computer-based monitoring, and presents few unique problems for the law.[65] Since service observation is by nature a method of intercepting the *content* of employee communications, legal rights to privacy under State tort law may be implicated, and while the employer often enjoys a qualified privilege to listen in on employee phone calls, that privilege may be vitiated by improper motive.[66] Otherwise, the employer's purpose for monitoring is not a consideration separate and apart from the manner and method in which the service observation is conducted.

Telephone Call Accounting

Chapter 3 discusses telephone call accounting in detail. Telephone call accounting systems are devices which can be attached to either the central office switch of the local telephone network or, increasingly, to the private branch exchanges (PBXs) on the customers' premises. Call-accounting systems generate detailed raw data on telephone usage; incoming and outgoing call numbers, total number of calls made, total time on the line, etc (they do not provide information on the content of the telephone call). This raw information can be processed by computer to provide summary reports of any type of telephone activity that the employer feels is relevant or useful.

Call accounting is often used for purposes that many might consider legitimate business functions, such as allocating costs between various accounts in a business, billing customers or clients for particular services, and keeping track of abuse or waste of local or long-distance telephone services. The recently enacted Communications Privacy Act of 1986 explicitly recognizes the need for call accounting in the course of providing communication services.[67]

The extent of personal phone use in the Federal Government was examined in a call-accounting audit conducted by the President's Council on Integrity and Efficiency (PCIE) in conjunction with the General Services Administration (GSA) and Office of Management and Budget (OMB). That audit reported in the fall

[65] A very important qualification to this statement is Title III of the Communications Act of 1934, which prohibits 'eavesdropping" per se, without regard to the intent of the person doing the eavesdropping, with certain crucial exceptions. Title III is considered more fully below under the manner and method analysis.

[66] "'[Defenses to common law claims of invasion of privacy include the defense of "privilege' The qualified privilege of the defendant to protector further his own legitimate interest has appeared in a few cases, *as where a telephone company has been permitted to monitor calls . . . ;* citing: *Schmulker v. Ohio Bell Telephone. Co.,* 116 N.E. 2d 819 (1953)(time and motion studies of employees); *People* v. *Applebaum, 97* N.Y. *S.* 2d 807 (1950) (tapping own telephone to protect own interests); *Wheeler* v. *Sorenson Mfg., 415* S.W.2d 582 (1967) (publication of wages and deductions of employees to combat union drive); and *City of University Heights v. Conley, 252* N.E. 2d 198 *(1969)* (spying on suspected thief). *Presser on Torts,* § 117

[67] The Electronic *Communications* Privacy Act of 1986, Public Law No. 99-508, 99th Cong., 2d sess., Oct. 21, 1986 *amends* portions of the criminal code (Title 18) to accommodate digital communications, computer networks, cellular telecommunications, and other advances in communications. Its import for telephone call accounting and service observation is discussed below where relevant.

of 1986 that on the average about 33 percent of long-distance calls made on the Federal Telephone System (FTS) were "unofficial," that is, made for personal reasons.

Concerns were raised in Congress over the implications of the PCIE audit for privacy and whistleblowing. Problems might also exist, particularly in the private sector, if call accounting were be used to frustrate union organizing efforts. As previously discussed, however, legal protections exist to address concerns over employee/union rights, and whistleblowers. Moreover, PCIE has adopted guidelines to address some of the concerns over the privacy and first amendment implications of the program.[68] Among the protections are: a "conservative" approach to classifying calls as "unofficial," prohibitions on invading the privacy of the persons called from the agency, categorization of 'calls possibly made to news media, congressional offices, public interest groups, and employee unions" as "official," [69] and a prohibition on using data to single out individuals or to conduct investigations.[70] It remains to be seen, however, whether and how the PCIE initiative will be continued and become part of the regular internal auditing Federal agencies. One department indicated that in spite of its pilot study results—indicating significant unofficial use of the department telephone system-the agency had no plans for further efforts to reduce these misuses, because of concerns over privacy implications.[71] If the audit does become a permanent part in intra-agency audits, questions arise over whether protective guidelines will also become permanent, and if so, how such guidelines will be enforceable. If, for example, a Federal employer were to discipline or withhold promotion or information from an employee based on that employee's contacts with the press, the employee may find it difficult to prove that the employer's motivations for doing so were the result of information obtained through telephone call accounting.

Although the PCIE study guidelines forbid listening to or recording conversations (as does Title III, discussed below), information on telephone transactions can yield a great deal of inferential knowledge about an employee's personal and life outside of work. Knowing that an employee contacted a particular newspaper one day before a damaging article is printed is sufficient to infer the content of the conversation, regardless of how that call is classified or whether it is subject to detailed investigation. Moreover, records of the audit which connect names and numbers, while protected by the Privacy Act, may nevertheless be subject to disclosure through the Freedom of Information Act.[72]

Yet another difficulty with the PCIE study guidelines concerns *enforcement and discipline*. At present the guidelines contemplate disciplinary action, such as removal, suspension, demotion, or reprimand only in cases of "extreme" cases of FTS abuse. The difficulty here is with selective enforcement and uniformit y of treatment. The PCIE guidelines offer no guidance on what constitutes "extreme" abuse, and no mention is made of who within each executive agency will be responsible for enforcement. This leaves considerable discretion to agencies' Inspectors General in determining who will be disciplined and under what circumstances. It opens the door to claims of differential treatment between low-ranking clerical staff and high-level government executives. Since the scope of job responsibility is often fairly narrow for low-level employees (e.g., claims processing at the Social Security

[68] General Services Administration, Office of the Inspector General, Office of Audits, "Guide for the PCIE Review of Federal Telecommunications System (FTS) Utilization, " part II, see especially app. XIII, pp. 65-74, July 3, 1985.

[69] Ibid., p. 29. Section IX of the "Guide" states that research activities concerning calls to these destinations should be terminated, that the information cannot be released to management, and that the information cannot be used against the person who made the calls.

[70] 1 bid., p. 30. The Guide does recommend, however, that "serious or egregious" cases of misuse should be referred to the agencies investigative organization for possible further action.

[71] OTA staff telephone interview with Department of Energy Office of Inspector General representative, fall 1986.

[72] See Title 5 U.S.C. §552, infra. See also Notice of Proposed Privacy Act Guidance for Call Detail Systems (OMB), 51 *Federal Register* 19982, 19984 (Friday, May 23, 1986), which discusses disclosure in the context of a permanent FTS telephone call-accounting system.

Administration), discriminating between "official' and "unofficial" calls may be relatively easy. But for high-ranking personnel, whose communications are more likely to be a mix of "business' and "pleasure, "7[3] such determinations may not be so easy. In other words, the informalities and ambiguities of the PCIE guidelines may give greater latitude to high-ranking employees than lower level employees. Under the proper circumstances, this may give rise to a claim of denial of equal protection of the laws under the 14th amendment.

Finally, there is a difficulty of *administering* the telephone call-accounting audit, particularly if it is implemented on a permanent basis. Although OMB has, under the PCIE guidelines, drawn up fairly extensive analyses of Privacy Act implications concerning employee privacy and the disposition of records, the question remains: who will be responsible for overseeing the agencies in the conduct of their audits to ensure that the guidelines are followed? A recent OTA report" concluded that OMB is not effectively monitoring such basic areas as: the quality of Privacy Act records; the protection of Privacy Act records in systems currently or potentially accessible by microcomputers; the cost-effectiveness of recordkeeping; and the level of agency resources devoted to Privacy Act limitations.

Such practical difficulties notwithstanding, there appears to be no dearth of legal protection for activities of Federal employees that the law recognizes as legitimate and responsible. However, the use of telephone call accounting by private sector employers for illicit purposes is not so clearly proscribed by law. In fact, the only recourse of the private sector employee against the employer for using call accounting to track whistleblowing activities is the nascent legal right against "wrongful discharge. "[75] Because of the principle of State action (see above), the private sector employee can claim no first amendment right to speak to the public or the press. Of course, statutes governing communications between employees and labor organizations, discussed above, apply with equal force to telephone call accounting. It should be noted that, unless the employer consents to the use of its telephones for labor organizational purposes, the employee probably does not have rights under statute to protest the use of telephone call accounting to track and squelch union communications.[76]

Manner and Method

Computer-Based Monitoring

The use of computer-based monitoring as a means for furthering the legitimate employer interests raises few, if any, legal issues. The first hurdle that an attorney challenging the practice itself must meet is to identify a' 'cause of action"—a legally recognized right that forms the basis for a lawsuit. The only right remotely relevant to monitoring is the right of privacy .77

Privacy is a broad value, representing concerns about autonomy, individuality, personal space, solitude, intimacy, anonymity, and a host of related concerns.[78] Since monitoring

[73]For example, is a long-distance call to set up *a* "business lunch" with a good friend an "official" or "unofficial" call?

[74]U.S. Congress, Office of Technology Assessment, *Federal Goverrnent Information Technology: Electronic Record Systems and* Individual Privacy, OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

[75]Retaliatory discharge for whistleblowing activities may be counter to public policy, and may thus constitute a wrongful discharge. See, e.g., *Monge* v. *Beebe Rubber Co,* 114 N.H. 130, 316 A.2d 549.62 A. L.R.3d 264,25 EPD P 31,643; and R. Murg and J. Sharman, "Employment at Will: Do Exceptions Overwhelm the Rule?" 28 *Boston College Law Review* 329 (1982). Moreover, employers may be held to their own internal statements of policy concerning matters such as privacy and treatment of employees with respect to monitoring. See, e.g., *Woolley* v. *Hoffman-LaRoche, Inc., 99* NJ 284,491 A.2d 1257 (1985), which held that the employer's official statement of policy for its employees created a contract of employment for an indefinite period.

[76]Under the National Labor Relations Act, 29 U.S. C. §158, for example, it is not unlawful for an employer to observe employee activities at the worksight during working hours to see if union activity is being conducted on company time. *IV. L.R.B. v. R.C. Mahon Co.* 269 F.2d 44 {6th Cir. 1959).

[77]Various theories under tort law, such as assault, intentioned infliction of emotional distress, defamation, outrage, and mayhem were considered, but lack sufficient connection to the types of activities involved in computer-based monitoring.

[78]See u S Congress, office of Technology Assessment, Fed*eral Government Information Technology: Electronic Record Systems and Individual Privacy,* OTA-CIT-296 *(Washington,* DC: U.S. Government Printing Office, June 1986).

is one method of obtaining information about and control over an employee's activities, some of these concerns may be relevant.

Although monitoring may affect culturally held values, there are serious problems in attempting to stretch the legally *enforceable* values regarding privacy, whether based on common law, statute, or the Constitution, to cover the types of monitoring considered in this report.[79] Although 34 States have adopted laws regarding employer use of polygraph machines, and 21 have laws addressing the privacy of employee records,[80] none have so far adopted legislation restricting monitoring, as such. One State, Massachusetts, has attempted to enact legislation that might prohibit computer-based monitoring per se, but the legislation was found to violate the due process and equal protection clauses of the U.S. Constitution.[81]

Furthermore, some State courts may hold employers to internal statements of policy regarding employee privacy, and may award damages for "unjust termination" of employees who seek to withhold information under these policy statements.[82] This approach has not been widely accepted in the courts, and the corporate policy statements seldom address monitoring explicitly.

There are several situations in which computer-based monitoring may implicate certain legal rights. The first is where the monitoring, which ordinarily reveals quantitative information about the amount of work done and the time spent doing it, reveals "personal" information as a byproduct. For example, if the only discretionary breaks allowed a monitored worker are for trips to the bathroom, the computer may allow an employer to glean this information by the frequency and duration that the employee is logged off the terminal.[83] In this situation, a breach of employee privacy is arguably present.[84] Another situation concerns the monitoring of personal computer use, and the auditing or editing of employee computer files. If the employer permits an employee to use computer files to store personal information, or electronic mail capabilities for personal messages, a breach of privacy may be found under a number of theories if the employer subsequently examines or reveals the contents of the files or mail.[85] Finally, to 'he

[79] The most widely accepted privacy framework under tort law is that offered by Presser. See "Privacy, 48 *California Law Review, 383 (1980).* Each of the four distinct torts–intrusion, disclosure, false light, and appropriation–require a physical invasion of the person or his/her property or personality and publication of the information gained by the invasion. Neither of these criteria is applicable to monitoring considered in this report. Moreover, consent to monitoring, either explicit or as a implied condition of the employment contract, would probably vitiate whatever claims an employee might have. Privacy under statutory law, at both the Federal and State level, concerns principally privacy of employee records, and while not relevant to the act of monitoring itself, may be relevant to records generated and kept by the monitoring system. This is considered below where relevant. Privacy under the U.S. Constitution has two main branches; rights under the 14th amendment, designed to protect family relationships, *Roe v. Wade*, 410 U.S. 113 (1973), *Griswold v. Connecticut, 381* U.S. *479 (1965);* and rights under the Fourth Amendment, designed to limit unreasonable searches and seizures. *Katz* v. *United States,* 389 U.S. 347 (1967), and progeny. Both of these branches require state action. Even supposing that monitoring might be considered a "search" under the fourth amendment, it is unlikely that an employee would be found to have a "legitimate expectation of privacy" in his or her performance at a given task. *Id.*

[80] These figures are from *Compilation of State and Federal Privacy Laws (1984-85* cd.), Privacy Journal (Washington, DC: Privacy Journal), and January, 1986 supp., but see: *Congressional Research Reports,* Mar. 21, 1986, which reports that 22 States have adopted laws regarding employer use of polygraph machines, and that 10 have adopted laws addressing employee access to records.

[81] *The legislation prohibited "the use of any monitoring device, without the express consent of the employee, by means of which the surveillance of employees might be effectuated. The term "monitoring device" included "any device, electronic, mechanical, visual, or photographic' by which 'appearance, actions, or speech" could be monitored. cite. *Re: Opinion of Justices, 356* Mass *756, 250* N.E.2d 448 ( ).

[82] *Op cit., Woolley v. Hoffman-LaRoche, 99* NJ 284, 491 A.2d 1257 (1985).

[83] See: Karen Nussbaum and Virginia DuRivage, "Computer Monitoring: Mismanagement by Remote Control, 56 *Business and Society Review* 16 (winter 1986); and Nine to Five: The National Association of Working Women, *Computer Monitoring and Other Dirty Tricks,* April 1986.

[84] The tort of intrusion may be applicable, if such monitoring amounts to an invasion of the employee's solitude or seclusion, even if there is not physical intrusion. Presser on Torts, p. 807. If the private activity is publicized, there may also be a tort for public disclosure of private facts.

[85] For public sector employees, an action may arise directly under the Constitution. For private sector employees, a tort action may lie. The Electronic Communications Privacy Act of 1986 is ambiguous as to whether an employer might access the contents of its employees' computer files. The prohibitions of the Act speak to an "electronic communication while it is in electronic storage." 18 U.S.C. §2701(a) (as amended). While perhaps not intended as a communication when written, all files in a personal computer are potentially communicable. Further, the Act's prohibitions do not apply to "the person or entity providing a wire or electronic communications service," or to

extent that the transactions monitored by computer become part of the employee's record of employment, compliance with procedures set out in the Privacy Act of 1974 (governing only Federal employees) or several State privacy statutes may be necessary.

Telephone Service Observation

Unlike computer-based monitoring, which primarily raises serious legal issues only when it is used to promote ends that are illegitimate, the legal difficulties with telephone service observation lie primarily in the manner in which it is carried out.

The principle law governing service observation is still Title III of the Omnibus Crime Control and Safe Streets Act of 1968, subject to the amendments involved in The Electronic Communications Privacy Act of 1986.X' Title 111 forbids the interception of the contents of telephone calls by government or private persons, except by judicial authorization. [87] This blanket prohibition on "wiretapping," however, is subject to two exemptions that permit telephone service observation—the consent and business extension exemptions.[88] Both exemptions have been construed narrowly by courts. Consent cannot be implied from the employee's knowledge of a capability for monitoring,[89] but must instead be based on a knowledge (or imputation of knowledge) that certain types of phones or phone conversations will be listened to.[90] Similarly, the business extension exemption applies only to the interception of particular calls as a part of the enterprise's ordinary course of business,[91] and even at that, one court has held that personal calls may be intercepted only to determine their nature, but never their content.[92]

Title III and the Electronic communications Act of 1986 appear to be the exclusive, albeit extensive, legal framework for issues that may emerge from telephone service observation.

Other legal theories, such as the common law right of privacy and (for governmental employees) the fourth amendment prohibition on unreasonable searches and seizures, while possibly forming the basis for a legal action, are unproven in the context of service observation. "A recent case held that, although public employees are protected by the fourth amendment, their expectation of privacy must be balanced against the government's need for supervision, control, and efficient operation of the workplace.[93] Moreover, the government is not held to a "probable cause" standard; instead, its actions are assessed under a "reasonableness under the circumstances" standard. Title III applied only to aural communications, but The Electronic Communications Privacy Act of 1986 extends the coverage of Title 18 to address analogous concerns present in the service observation of the content of data communications.[94]

---

a "user of that service with respect to a communication of or intended for that user. 18 [J. S.C.§2701(b) (as amended).

[87] "l-itlt' 111 of the Omnibus Crime Control and Safe Streets Act, 1 8U.S.C. §§ 25102520 (1976). Public Law No. 90-351, § 802,82 Stat. 212, as amended by The Electronic Communications Privacy Act of 1986. Public Law No. 99-508, 99th Cong. 2d sess., Oct. 21, 1986.

[88] The relevant portion reads:

> Except as otherwise specifically provided in this chapter any person who --
>
> (b) willfully uses, endeavors to use, or procures any other person to use of endeavor to use any electronic, mechanical, or other device to Intercept any oral communication.
>
> shall be fined not more than $10,000 or imprisoned not more than five years, or both
>
> 18 U S.(. §251 1(I)(b).

The statute also provides for a civil remedy and statutory damages. 18U.S.C. 12520.

"Section 251 1(2)(d) of the law permits interception "where one of the parties to the communication has given prior consent to such interception, and Section 251 l(l)(b) excludes from coverage "any telephone or telegraph instrument, equipment or facility, or any component thereof. . . .being used by the subscriber or user in the ordinary course of its business; .' I n addition, communications common carriers may "intercept, disclose, or use (an employee's telephone conversations) in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication . . ." 18 U.S.C.§251 l(2)(a)(i).

[89] *Watkins v. L.M. Berry & Co., 704* F.2d 577 (11th Cir.1983); *Campiti v. Walonis, 611* F.2d 387 (1st Cir.1979); *Crooker v. U.S. Department of Justice, 497* F. Supp. 500 (D.Corm, 1980),

[90] *Watkins v. L.M. Berry, supra*; *Jandik* v. *Village of Brookfield, 520* F. Supp. 815 (N.D. Ill. 1981).

[91] *Watkins* v. *L.M. Berry &* Co., *supra*; citing *Briggs* v. *American Air Filter Co., 630* F.2d 414 (5th Cir.1980).

[92] *Watkins v. L.M. Berry & Co., supra* at 583. 1 n essence, the court held that, once the personal nature of the call is known, the employer must hang up.

[93] *O'Connor* v. *Ortega, 107'* S. Ct. 1492.55 USLW 4405 (19871.

[94] Title I I I convered only oral communications, 18 U.S.C. §2510., *cf. U.S. v. New York Telephone Co., 434* U.S. 159(1977) holding that a communication under Title 111 must be capable of being overheard.

Telephone Call Accounting

Many of the legal issues surrounding the use of telephone call accounting center on the incidental information generated by a call-accounting system. In other words, although the employer may not purposely set out to infringe employee rights, many of the by-products of call-accounting systems may in fact threaten employee privacy. In the act of tracking recipients of calls originating from certain phone numbers, employers must, of necessity, obtain information on the identity of the persons called, and the nature of the call (business or nonbusiness). Depending on how the audit is conducted, and how closely focused on individuals it is, a' 'picture' of extra-employment activity may be obtained merely from the identity of the destination phone numbers, even if the intent of the audit is to identify nonbusiness-related calls.[95] Once the information is collected, it maybe intentionally or accidentally disclosed to people whom the employee would prefer remain unaware. Although a call-accounting audit may disclose misuse, such misuse may not be the fault of the employee (especially when others have access to the employee's phone)–a claim that maybe hard to prove.

Federal employees are the most protected segment of the labor force. If the records generated by the telephone call-accounting system form part of a "system of records" personally identifiable to particular individuals, then, under the Privacy Act of 1974, the Federal employee is subject to a number of procedural safeguards concerning notice that such records are being collected, the subsequent use to which they can be put, the right of the employee to corrector amend the records, the necessity, and the acquisition for lawful purposes of those records.[96]

For public employees in general, it is unlikely that a constitutional claim under the fourth amendment could successfully be brought against the practice of telephone call accounting—even against its surreptitious use by police in order to obtain evidence for a criminal indictment .97 The Electronic Communications Privacy Act of 1986, while providing stronger protection than the fourth amendment by requiring a court order for the application of pen registers and trap and trace devices, 98 is applicable to telephone call accounting.[99] However, depending on how the information gleaned from call-accounting systems is used and whether it is disclosed, all employees may have rights under common law theories of privacy or defamation.

Effects

Aside from the abusive purposes and methods of electronic monitoring discussed above, the most salient legal issue presented by monitoring concern its health-related effects on particular workers. Other, less tangible, effects

[95] Calls to collection agencies may reveal debt trouble; calls to counselor may reveal psychological or marital trouble; calls to employers in similar businesses may reveal an intent to change jobs; and calls to the news media may reveal the source of "leaks."

[96] 5 U.S.C. §552(a), *infra*.

[97] Pen registers, which are devices that attach to a telephone line to record dial pulses, may be used in law enforcement to obtain information on suspects without the need of a search warrant. *Smith v. Maryland, 442* U.S. 735 (1980). By extension, the use of call-accounting systems (that achieve very much the same result-albeit, in a more detailed fashion), which often form an integral part of modem PBXs, would seem to raise no unique fourth amendment problems, especially when they are used on the employer's premises and it is known by employees that they exist (thus raising no "subjective expectation of privacy").

[98] 18 USCCh. 206 "Pen Registers and Trap and Trace Devices."

[99] Title 18 has been amended so as to specifically exclude a "provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed *in order to protect* such provider, another provider furnishing service toward the completion of the wire or electronic communication, or *a user of that service, from fraudulent, unlawful, or abuse use of such service; " 18* U.S.C. 2511(3)(h)(ii) (emphasis added).

Call-accounting software might arguably be a "pen register" for purposes of The Electronic Communications Privacy Act of 1986, since, like SMDR PBX equipment, it is defined as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such devices is attached. . . ." However, SMDR equipment and software is excepted from the prohibitions of the act: "(pen register) does not include any device used by a provider or customer of a wire or electronic communication service *for billing, or recording as an incident to billing*, for communications services provided by such provider or any device used by a provider or customer of a wire communication service *for cost accounting or other like purposes in the ordinary course of its business . . ."* 18 U.S.C. $3126 (emphasis added).

are sociological in nature, and concern the impact of monitoring on the overall climate of work in the United States.

The literature on stress and work monitoring is not broken down cleanly into the three categories of monitoring dealt within this report. Computer-based monitoring, telephone service observation, and telephone call accounting may each entail widely different work environment factors (e.g., different organization factors, different physical relationships be tween the employee and the technology on which the employee is working, and different expectations). Thus, any particular findings on stress are likely to vary widely between types of work monitoring. Nevertheless, most of the legal analysis that follows will hold true so long as stress can be shown to be caused by or associated with the particular type of monitoring in question.

This section relies on the analysis developed in chapter 2 examining the evidence for computer monitoring as a cause of stress, and applies relevant law in fight of this evidence. The principle conclusions of chapter 2 are: 1) that evidence that computer monitoring, per se, causes stress is suggestive, but not conclusive; and that 2) many other aspects of job design and work enviornment-e.g., computer pacing, heightened work pressure, routinized activities, variable workloads, lack of control over the task, lack of decision latitude, lack of peer and supervisory support, and fear of job loss—may also cause stress among VDT office workers. Research to date has not succeeded in separating the effects of computer monitoring from effects of these other workplace factors, insofar as stress is concerned.[10]

Many of those opposed to work monitoring focus on its health, and particularly stress-related, effects. Moreover, many of the "case studies" submitted to OTA by a variety of unions emphasize the deleterious effects that monitoring has on employees' health. The approach of this section will therefore be to take the assertion that monitoring causes stress and health-related problems as a given, and ask: how might present law address concerns over these effects of monitoring?

All State jurisdictions recognize stress as a compensable injury, either under their tort or Worker's Compensation laws.[101] However, "stress" is subject to a wide variation in definition in the way it is manifested, and the manner and context in which it is inflicted. Standards of proof for its existence, and the degree of injury necessary for compensation, are determinative of whether monitoring-induced stress (if it can be shown to exist) will rise to the level of a legally recognized claim.

Worker's Compensation, which was established in all 50 States to provide compensation on a "no-fault" basis for the loss of ability to earn wages, is a substitute for employer tort liability. Most Worker's Compensation statutes require that the injury be accidental, and that it arise out of or in the course of employment. Courts have read these requirements expansively in recent years, so that even "accidents" that are slow in manifestation and which rise out of employment-related risk are compensable.[102] This means that, as a threshold matter, chronic stress caused as a result of monitoring may be compensable.

[100] Stress due to work monitoring should be considered separately from that due to the use of Video Display Terminals (VDTs) per se. A recent OTA report concluded that "evidence for a relationship between stress-related disease and VDT work is still sparse." U.S. Congress, Office of Technology Assessment, *Automation of America Offices, OTA-CIT-287* (Washington, DC: U.S. Government Printing Office, December 1985), p. 150. In part, this is due to the methodological problems in attributing stress and stress-related ailments to any one factor or combinations of factors in the workplace. The OTA report did conclude, however, that electronic monitoring in general is associated with the symptoms of chronic arousal, and can lead to increased anxiety, fatigue, psychosomatic complaints, and job dissatisfaction. *Id.* at p. 130. In this regard, the report did not separate computer-based monitoring from customer service observation and call-accounting systems, as is done in this report. However, the way in which monitoring was described, as a system of electronic supervision or feedback in work organization, would include the first two forms of monitoring considered in this report. Moreover, machine pacing—the use of a computer to control when and how fast a task is performed—can lead to anxiety, depression, boredom, dissatisfaction, frequent health complaints, and decreases in productivity with increases in error rates. *Id.* at 128-29; citing Salvendy and Smith (eds.), *Machine pacing and Occupational Stress (London: Taylor & Francis, Ltd., 1981).*

[101] 1B Larson, The Law *of Workmen Compensation,* §42 *infra (1982),* and Presser, *Law of Torts,* $12.

[102] 1 A Larson, The *Law of Workmen's Compensation. 5$37.00-39.00* and $$6.00-8.00, *infra*

Even if stress meets these threshold requirements, not all States recognize psychological effects as compensable injuries caused by stress. [103] Only a handful of States would allow recovery for monitoring-induced stress, if that stress can be characterized as "not unusual, ' ' or "not in excess of everyday life or employment. "[104] Otherwise, in order to be a compensable injury under Worker's Compensation laws, stress must be "unusual, "[105] or even "sudden," "frightening," or "shocking. "[106] As electronic monitoring gains acceptance as an ordinary part of the work environment in which it is deployed, any stress that it causes (if any) is arguably "not unusual. " In order to be recognized in most States, therefore, electronic monitoring-induced stress must manifest itself in a physiological symptom to be compensable.

Finally, many States today recognize the tort known as "intentional infliction of emotional distress. " Although compensation for emotional distress previously required some sort of physical invasion or injury, such as a battery or assault, this is no longer the law in a substantial number of jurisdictions. This notwithstanding, monitoring-induced stress is unlikely to be actionable under tort law. First, the distress-producing act must often be of an "extreme and outrageous" nature—a characterization that is probably not fitting to electronic work monitoring. Secondly, as with the tort of invasion of privacy, consent (found in the implied or explicit terms of an employment contract) will probably vitiate an employee's claim. Finally, many States still require that physical illness or some other nonmental effect be present before allowing recovery.

[103] Florida, Georgia, Kansas, Louisiana, Minnesota, Montana, Nebraska, Ohio, and Oklahoma do not recognize purely mental or emotional injuries as the result of stress. *Emotional Stress in the Workplace,* op. cit. All jurisdictions recognize stress-related ailments, whether "mental" or "physical," that have an antecedent physical injury. And, with the exception of Ohio, all States recognize "physical" disabilities resulting from stress. 1A Larson, §42.22 et seq.

[104] California, Hawaii, Kentucky, Michigan, New Jersey, Oregon, and West Virginia. See generally "Emotional Stress in the Workplace–New Legal Rights in the Eighties, National Council on Compensation Insurance, 1985.

[105] Arizona, Arkansas, Maine, Massachusetts, New Mexico, New York, Pennsylvania, Rhode Island, Washington, Wisconsin, and Wyoming. *Id.*

[106] Illinois, Maryland, Missouri, Mississippi, South Carolina, Tennessee, Texas, Virginia. *Id.*

PART IV: CONCERNS NOT ADDRESSED BY LAW

Table 16.—A Framework for Addressing Electronic Work Monitoring

	Concern	Criteria	Example of applicable law	Possible "gaps" in law
Purpose of monitoring	Fairness	Relevance Completeness Targeting	National Labor Relations Act; Civil Rights Act; Merit System Principles (as administered in EEO, OSHA, ERISA, EPA, etc.[a]); State Law on Privacy; Constitutional Law[a]	Due process—type guidelines for private employees
Manner and method of monitoring	Autonomy Dignity Privacy	Intensiveness Intrusiveness Visibility Type Leakiness Permanence	State Law on Wrongful Discharge; State Law on Privacy; PCIE Guidelines; Title III of Omnibus Crime Control and Safe Streets Act; Electronic Communications Privacy Act; National Labor Relations Act; Privacy Act of 1974[a]	Privacy in transactional information; "Human Rights"—type law; laws requiring notice of monitoring
Effect of monitoring	Health Stress	Frequency Continuousness Regularity Control	Worker's Compensation Statutes on Stress-Causing Labor	Guidelines/regulations on stress—inducing labor practices

[a] Applies only to Federal employees

SOURCE Off Ice of Technology Assessment, 1987

If we look at the types of concerns raised by electronic monitoring, and at those addressed by law, several broad conclusions follow:

Purpose

- In general, public *employees are better protected against "unfair' monitoring practices than private sector employees.* Constitutional due process protections afford public sector employees the opportunity to challenge dismissals, demotions, or other actions based on monitoring that is irrelevant, unfairly targeted, or incomplete. Although the doctrine of employment-at-will is gradually being eroded in State courts, a suit for unjust dismissal of private sector employees based on unfair monitoring is unlikely to succeed.
- Aside from provisions made in union contracts, *no law compels an employer to implement monitoring with fairness,* unless it can be shown that the employer has taken actions against certain employee(s) based on race, sex, or religion or for motivations that are against narrow public policy exceptions to the employment-at-will doctrine.
- • *Electronically monitoring formerly unmonitored tasks may change the very nature of that task, by accommodating the task to the system of measurement.* While some employees may object to this as an unbargained for change in job description, no legal protections, aside from employment contracts, exist.

Manner and Method

- Monitoring most often involves the collection of transactional, rather than substantive, information about employees' performance. No privacy *protections exist against the* collection *of transactional information on employees activities while at work.* For example, no law prevents the collection of telephone usage data in a call-accounting system, or of performance data in a computer-based monitoring system. If, however, transactional data becomes part of a personally identifiable *record,* then the *subsequent use and disposition of that record is regulated by both Federal and State law.*
- *With some exceptions, no law prevents an employer from using the monitoring systems considered in this report in a secretive, low visibility manner.* For example, an employer is not under a positive duty to reveal to its employees the fact that their keystrokes are being counted, or that their outgoing long-distance calls are being documented. Unless the employee has an expectation of privacy in the activity or location while at work, the employer is free to collect as much information on the employee performance as it sees fit.
- Although employees may regard some methods of monitoring as an assault on their dignity or autonomy, *there is no legal right to be treated with dignity or as an autonomous person.* Unless the monitoring technique is intrusive—invading either the bodily *or* mental integrity of the person (as, perhaps, in drug testing or brain wave analysis)—there are no legal protections against monitoring because it is "dehumanizing." Although monitoring may affect interpersonal and power relationships at work, no law prevents employers from using intense, low visibility monitoring. For example, using computers to set the pace at which tasks are accomplished, to measure the employees' performance, or to document time away from a terminal, are not prohibited by law.

Effects

- Although some forms of monitoring *may* cause stress, and *may* therefore have health effects, *no law currently protects workers against stressful environments,* whether the stress is caused by monitoring or by other aspects of the work environment. Lawmaking with respect to stress in the work environment is not unprecedented, however, and several foreign countries have adopted legislation that attempts to address stress in the work environment.

- In some cases, *stress may be a compensable injury under Worker Compensation statutes,* but stress-related health effects are difficult to prove, and are not accepted in a majority of State courts.

What Does the Future Hold?

Depending on the influence of a variety of business, economic, and social factors (see part II), the next 10 to 15 years may see substantial changes in monitoring technologies and settings in which they are conducted. These changes may raise a whole new set of concerns warranting continued congressional scrutiny.

Incremental Changes

Today's monitoring techniques, which are in and of themselves neither illegal nor clearly in conflict with employer-employee custom, necessarily form a precedent for future monitoring techniques. As these techniques become more sophisticated and permeate the work environment, law and lawmakers may have a difficult time distinguishing between each new innovation and the one that preceded it. The law and practice that grows up around a particular form of monitoring may easily assimilate anew, incremental change in the technology or application. The cumulative changes in work environment may be great, despite their gradual and hence imperceptible nature. The framework for analyzing claims to privacy, which relies on an assessment of an individual's "reasonable expectations, " 107 can easily become simple descriptive statements of what the monitoring milieu *is,* rather than prescriptive statements of what *ought to be.* An individual's knowledge that certain technologies are capable of intruding into previously private realms may vitiate claims that the individual's expectation of privacy was a reasonable one.[108]

Work Environment Changes

Much of employee behavior in the past went unobserved or undocumented simply because the technical facility for monitoring it did not exist, or was too cumbersome to employ. As noted in chapter 2, however, the use of modern information technology enables employers to keep track of more information on employee performance in much greater detail. Given this new ability, much of the "looseness" of previous work environments may be reduced or eliminated. What was in the past a de facto perquisite of the job, such as a limited ability to make nonwork-related phone calls, or an occasional break from a given task, may in the future become grounds for discipline or dismissal. In such a case, the question is not whether the employer is "within his rights, " but whether the work environment should become so rigorously controlled as to eliminate all discretionary employee activity.

Qualitative Changes

As discussed elsewhere in chapter 1, a clear distinction can be made between work monitoring and worker testing; the former is an evaluation of the performance or behavior of an employee, while the latter is an evaluation of an employee's physical or mental state. In theory, it maybe possible for legal rules to be framed in accordance with this distinction. However, while the distinction may be relatively easy to make in theory, it is breaking down in fact. Research in the field of psychophysiology, discussed elsewhere in this report, may be able to correlate behavior with psychophysiological states; blurring the boundaries between monitoring work and monitoring the worker.

[107] *Katz* v. *Urn-ted States,* 389 U.S. 347 (1967) announced the constitutional "reasonable expectation of privacy" standard that has guided the Supreme Court ever since. It has two components: whether the individual actually expected that his or her activity remain private, and whether that expectation is one that society is prepared to accept as reasonable. This standard has gradually been applied in nonconstitutional, tort-privacy cases.

[108] For example, in *California V. Ciraolo, a* recent case in which police used an aircraft and camera to obtain evidence of marijuana growing in a suspect's backyard, the Court concluded that "[t]he Fourth Amendment simply does not require the police traveling in the public airways . . . to obtain a warrant in order to observe what is visible to the naked eye. " The standard for determining what expectations of privacy are reasonable is, in part, dependant on the state of technology for intruding on that privacy.

PART V: POLICY OPTIONS

Before addressing the problem of how Congress might act, it is first necessary to consider *whether* and *when* action may be appropriate. Some factors suggest that a "wait and see' posture may be appropriate; uncertainty about whether monitoring causes stress, the lack of judicial precedent, the possibility of privately negotiated restraints on monitoring, and marketplace checks on monitoring are among these. Other factors indicate that Congress may want to act now to alleviate growing concern about monitoring in the workplace. These include the lack of union representation in the bulk of the monitored work force, inadequacy of current law to address concerns over health, privacy, and dignity, difficulties of legislating against powerful economic interests at the State level, and increasing sophistication of the technology itself. Several possible directions of Federal policy are described below.

Option 1: Take no Federal action concerning work monitoring at this time.

Questions of the fairness of work monitoring practice would be left, as they are at present, in the hands of stakeholders, employers and employees. In industries where labor unions are active, collective bargaining with regard to technology change, monitoring, and methods of evaluation should continue under current rules.

Although many unions have adopted positions opposing electronic work monitoring (see table 11), their bargaining strength with respect to it, whether by informal negotiations or by formal collective bargaining or arbitration, is probably not great. However, some forms of monitoring take place within specific industries or companies. An argument can therefore be made that, pending the development of a longer history of negotiations between labor and management on this issue, monitoring is best addressed at the union level; the parties concerned are most familiar with the specific problems, and contracts, rather than national policy, are the best way of approaching what appears to be situation-specific problems (see part III). Under these circumstances, Congress may want to avoid legislating on the issue of monitoring per se, and instead make monitoring an item for compulsory arbitration or collective bargaining under Federal labor law.

This, of course, does not necessarily ensure an outcome that is satisfactory for the majority of monitored workers, who are not unionized and are therefore powerless to negotiate a fair monitoring practice, or any other aspects of the quality of work life, through the collective bargaining process. Furthermore, a growing segment of the work force are temporary workers, who, since they come and go on a weekly or monthly basis, have little ability to improve the quality of worklife.

There is the argument that natural "market forces" may tend to limit unfair monitoring and preclude the need for congressional action even on behalf of nonunionized workers: employee backlash, low morale, and high turnover should dissuade employers from monitoring practices that their workers find onerous. If monitoring is indeed stress-producing, then employers who use it will inevitably see the effects of stress on diminished quality and output of its product or service. The response to this is that many monitored jobs comprise routine work subject to and indifferent to a high turnover rate. And, in many instances, high attrition works to the employer's benefit (by lowering the costs of pension, salary increases, etc.). Thus it is not clear that "natural' checks will be sufficient to ensure that monitoring is not abused.

If natural checks are not sufficient, political action is still available. Unions and other interest groups have worked to pass State level legislation on monitoring, service observation, or VDT health and safety. These activities will probably continue. Some of these attempts may be successful, giving rise to a variety of legislative or regulatory approaches to deal-

ing with issues related to electronic monitoring. Some may serve as models for Federal action at some later time, should the need for the harmonizing effect of national legislation be seen more clearly in the future.

Option 2: Establish whether stress effects of electronic monitoring are an occupational health hazard; if they are, consider creating Federal legislation or regulations governing the use of electronic monitoring.

The effect of monitoring on stress and health-issues which might provide the policymaker with the most direct and least value-laden approach to acting on monitoring–is in a state of scientific uncertainty. There exist few authoritative studies on the effects of electronic monitoring on health. Many studies and informal polls of workers suggest that monitoring has stressful effects, and there is a certain common sense appeal to the idea that working in fast paced, highly monitored environments may be very stressful. However, not much is known about the types of monitoring that are stressful, how stress might be reduced, or how stress due to monitoring manifests itself (if at all) in physiological symptoms. Until more is known about the effects of monitoring on health, policy action under a "stress" rationale may be premature. The policy maker may consider it appropriate, therefore, to initiate studies on stress in the workplace, and on the role that monitoring plays in such stress.

The National Institute of Occupational Safety and Health would seem to be the logical agency to supervise or carry out studies of stress as a workplace hazard. Specific studies of monitored workers would have to be done with an eye to understanding the effects of monitoring independent of other workplace stressors, a major deficiency in existing studies. In addition, however, it would be useful to understand more about the phenomenon of workplace stress in general, given the rising number of worker compensation claims and other evidence of the growing importance of stress in occupational health. Research may reveal that other factors in the workplace are as important as or more important than monitoring in contributing to stress-related illness, and that these should also be covered by protective legislation or regulation.

Option 3: Consider Federal legislation aimed at gaps in current law. This could be in two possible directions: general legislation aimed at establishing certain rights for employees within the workplace or surgical legislation aimed at specific monitoring practices.

There have been *no* court cases challenging the types of monitoring considered in this report. Two conclusions can be drawn from this. The first is that, until the judiciary acts, Congress has very little clue (aside from analyses of the sort found in part III of this chapter) as to the type of legal inadequacies it should address, and ought therefore to wait to legislate on work monitoring. The second is that current law is inadequate to even form the basis for a lawsuit, and that Congress must take the lead in providing rights to monitored employees, should it decide that certain forms of monitoring are pernicious.

Current worker protection legislation gives workers a variety of rights, such as the right to organize, to bargain collectively, to minimum wage, and increasingly, the right to know about health and safety hazards that form part of the working environment. However, U.S. law has not heretofore involved itself deeply in quality of worklife issues nor in issues of personal privacy or dignity in the workplace. There is no legal right to be treated with dignity or as an autonomous person. There is no legal right to a well-designed, interesting job, nor is there law that compels employers to consider employee input in decisions about new technology or new monitoring procedures. To the extent the law treats privacy in the workplace, it looks to a standard of what an employee might reasonably expect to remain private; as mentioned earlier in this chapter, this standard may fail as a guide for action in the face of employer's increasing use of monitoring, surveillance, or testing technologies.

That these issues are not currently addressed in law does not mean they could not be. As is discussed in appendix A, a number of other countries have quality of worklife legislation. Such legislation could give guidelines on the rights to health, safety, privacy, constitutional protections, or information that employees can expect to enjoy in the workplace. As indicated earlier in this chapter, the erosion of the doctrine of "employment-at-will" through anti-discrimination, health and safety legislation, and public interest concerns, has already marked some involvement of the U.S. Government in regulating the work environment. The issue of electronic monitoring in offices is too narrow to serve as a basis for comprehensive work environment legislation. It should be just one factor of many to be considered in determining what rights U.S. citizens have in the workplace, both as employers and employees.

However, assuming that blanket legislation on worklife quality is neither wise nor desirable, Congress might address concerns over specific issues through the use of specific amendatory legislation. If, for example, telephone call accounting is an area of particular concern, Congress might address the problem specifically by amending the Electronic Communications Privacy Act to comport with what it considers "fair" monitoring practice. The President's Council on Integrity and Efficiency guideline may form a template for such legislation, or instead, Congress may mandate alternatives to telephone call accounting discussed in chapter 3 of this report.

Another example of an area of the law not currently addressed, and on which Congress may wish to act, is what might be called transactional privacy, or the collection of "information about information. " For example, the number of keystrokes, the number of visits to the bathroom, the destination of calls, etc., are all type of information about transactions, rather than about the content of communications or activities (see part II).[109] Although present law, such as the Privacy Act and the Fair Credit Reporting Act, regulates what can be done with transactional information once collected, it does not forbid its collection as such. As we have seen, however, the collection of transactional information, particularly if done on an intensive basis (see part II) can arouse feelings of having one's privacy, dignity, and autonomy invaded. Moreover, because of the power of computers to generate profiles and crosshatch many transactions, transactional information can yield informed estimates of the substantive content of communications or patterns of behavior—it can be, in other words, a "back door" for getting at personal information that existing law regulates.

Certainly, to forbid or regulate the collection of all transactional information would be unreasonable. Much transactional data collected by electronic monitoring software is used to monitor equipment utilization, to track totals of transactions made, and to determine whether security systems are working properly. The collection of transactional data becomes most subject to controversy when it is collected about the performance of an individual worker. It maybe that Congress would choose to treat electronic monitoring as a' 'right to know' issue for workers; that is, employers could have the right to collect whatever kind of transactional data they wish about employee performance, but would be required to give employees access to, and if need be, correct, this information.

As this report has indicated throughout, however, the issue of work monitoring cannot be adequately understood, nor appropriately addressed, in isolation from larger labor-management, privacy, and the health and safety context in which it is embedded. Nor will specific policy actions taken with respect to particular forms of monitoring necessarily end the controversies arising out of the application of new technology forms in the workplace. The policy maker should therefore be aware that an exclusive focus on the forms of monitoring considered in this report will at best form the basis for a series of patchwork solutions to what has been a perennial issue between workers and employers.

[109] *Transactional* information, it will be recalled, differs from *substantive* information, in that the latter reveals the content or meaning of communications or documents. Transactional information, in contrast, reveals facts about communications or documents.