Chicago-Kent Law Review

Volume 72
Issue 1 *Symposium on Generic Products Liability*

Article 9

January 1996

Privacy in the Workplace: How Well Does American Law Reflect American Values?

Alan F. Westin

PRIVACY IN THE WORKPLACE: HOW WELL DOES AMERICAN LAW REFLECT AMERICAN VALUES?

ALAN F. WESTIN*

INTRODUCTION

Examination of the issue of privacy in the workplace presents two basic questions for discussion:

- What are (or should be) the legitimate privacy rights of employees in the work world of the late 1990s?
- How does (or how should) American law balance employee-privacy claims against competing employer and societal interests in information disclosure and protective surveillance?

These questions can be applied to each of the major arenas of workplace privacy: pre-employment information collection; on-the-job information practices; and employer use of off-the-job information. Indeed, there are whole treatises and loose-leaf services that cover these arenas of employee privacy in detail.[1]

In this Article, I explore the interplay of three factors that I believe fundamentally shape the way our society treats all privacy issues, including workplace privacy:

(1) the balance that contemporary society sees as desirable for organizational-individual relationships in a given sector (such as banking, health care, or employment);

(2) public perceptions of what are reasonable and unreasonable expectations of privacy in that setting; and

(3) the public's sense of appropriate and inappropriate mechanisms or remedies to protect privacy interests.

To pursue this analysis, I start by summarizing briefly what two decades of survey research tell us about the public's concerns about

* Professor Emeritus of Public Law and Government, Columbia University; Publisher, PRIVACY AND AMERICAN BUSINESS; Author, PRIVACY AND FREEDOM (1967).

1. *See* JON D. BIBLE & DARIEN A. MCWHIRTER, PRIVACY IN THE WORKPLACE: A GUIDE FOR HUMAN RESOURCE MANAGERS (1990); EDWARD F. DOLAN, YOUR PRIVACY: PROTECTING IT IN A NOSY WORLD 64-90 (1995); MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW (BNA, 1995); RONALD M. GREEN & RICHARD G. REIBSTEIN, EMPLOYER'S GUIDE TO WORKPLACE TORTS (1992); L. CAMILLE HEBERT, EMPLOYEE PRIVACY LAW (1996); MARVIN F. HILL, JR. & JAMES A. WRIGHT, EMPLOYEE LIFESTYLE AND OFF-DUTY CONDUCT REGULATION (1993); INDIVIDUAL EMPL. RIGHTS CASES (BNA loose-leaf service); WILEY EMPLOYMENT LAW UPDATE (Henry H. Perritt ed., 1995).

privacy in America, the social forces and values that are driving these public concerns, and the way that a majority of Americans seem to go about deciding what are proper and improper uses of their personal information. In my view, the body of survey research on privacy that has been built up over the past twenty years is a major—and much under-utilized—resource for considering policy issues and legal options with regard to privacy issues.

Turning to workplace privacy, I summarize what the survey research tells us about employee perceptions of employer information practices in the 1990s. Then, I apply these findings about majority values, privacy balances, and the role of law to the currently hot issue of worker monitoring.

PUBLIC VIEWS OF PRIVACY: AN OVERVIEW

Eighty-two percent of the American public said in 1995 they are "concerned today about threats to their personal privacy."[2] This is up from thirty-four percent in 1970, sixty-four percent in 1978, and seventy-nine percent in 1990.

In the broad area of consumer privacy, eighty percent of Americans say that "consumers have lost all control over how personal information about them is circulated and used by companies." This is up from seventy-one percent who felt that way in 1990. Consumers say they are resisting intrusive information collection wherever possible. Fifty-nine percent report that they have "refused to give information to a business or company because [they] thought it was not really needed or was too personal," up from forty-two percent in 1990.

Harris surveys from 1978 to 1995 confirm that these and other concerns about privacy do not follow any pattern of standard demographics, such as age, education, income, race, gender, community, section, or political philosophy. Rather, they are closely correlated with and basically driven by two factors—strong majority distrust of public and private institutions and fears of technology abuse. Since distrust levels in American society in 1996 remain intense, we should not expect worries about privacy threats to subside soon.

At the same time, the surveys show that the American public takes a pragmatic approach to the resolution of concrete privacy issues. Only twenty-five percent of the public displays what can be

2. LOUIS HARRIS & ASSOCS. & DR. ALAN F. WESTIN, THE EQUIFAX-HARRIS MID-DECADE SURVEY ON CONSUMER PRIVACY (1995).

called "privacy fundamentalist" views, while about eighteen percent of the public is "privacy unconcerned." A majority—fifty-seven percent—are what I have called "privacy pragmatists." In the consumer area, they will look at calls to provide businesses with their personal information to see whether they feel that they will get a desirable benefit or opportunity by complying. If so, they next look to see whether the business follows fair information practices that will protect the privacy and confidentiality of their information. If this is done, the privacy pragmatists supply their information, and accept this as a fair exchange, joining the privacy unconcerned to make up a seventy-five percent majority.

But, if the privacy pragmatists do not feel a valuable benefit or opportunity is being offered, or that fair information practices are not assured by law or provided by voluntary organizational policy, most will join the privacy fundamentalists, creating an eighty percent level of opposition to that information practice.

These pragmatic views are reflected in positive majority attitudes toward the value of the credit reporting system for rapid and broadbased consumer access to loans, retail credit, and credit cards; in approval of marketers providing opt-out (rather than opt-in) procedures for customers who do not want to receive offers of additional goods or services from businesses they patronize; and in support for financial institution affiliate sharing of consumer information for offering customers other financial and nonfinancial products.[3]

In addition, the U.S. public generally prefers voluntary privacy policies to government regulation. Seventy-two percent of the public agreed in 1995 that "if companies and industry associations adopt good voluntary privacy policies, that would be better than government regulations, in this country."[4]

Finally, the European model of government data protection boards with jurisdiction over the private sector and systems of registration of every data base with personal information with a supervisory government registrar has never drawn a majority of public support in the United States. In the present atmosphere, most Americans see that approach as calling on "Big Brother" to protect citizens from "Big Brother."

3. *See* LOUIS HARRIS & ASSOCS. & DR. ALAN F. WESTIN, CONSUMERS AND CREDIT REPORTING (1994) (survey sponsored by VISA and MasterCard).

4. HARRIS AND WESTIN, *supra* note 2.

PUBLIC VIEWS OF WORKPLACE PRIVACY

Given such high levels of concern about consumer privacy (matched by concern about privacy of medical records),[5] and judging from widespread media stories about intrusive employers and threats to employee privacy rights, one would expect surveys of employees to record high levels of concern and perceptions of abuse. But this is not so.

In 1993, as background for a documentary on public television about privacy and collection of health information about employees, Harris did a detailed survey of one thousand persons working in private sector companies with fifteen or more employees, asking both general questions about workplace privacy issues and specific questions about the highly-sensitive area of medical and health information collection by employers. At the same time, three hundred human resources executives in private sector companies were surveyed on the same issues.[6]

The results surprised many privacy experts:

- Ninety percent of employees said that their employer had *never* asked for personal information they thought was inappropriate because it was not needed for the employment relationship and its administration.
- An identical ninety percent said that their employer respected the off-the-job privacy of employees, with sixty-one percent saying off-the-job privacy was "very well" respected.
- Less than one in ten employees—only eight percent—thought their employer had collected information about their health or lifestyle off the job that should not have been collected.
- And, ninety-four percent said they did not know of any occasion when their employer had *ever* used personal information about them unfairly.

These extremely high levels of employee confidence in employer collection and uses of information take on considerable weight because this same sample of private-sector employees displayed identical levels of deep concern about *citizen* and *consumer* privacy as samples of the overall public. For example, when asked how concerned they were about threats to their personal privacy in America

5. *See* LOUIS HARRIS & ASSOCS. & DR. ALAN F. WESTIN, HEALTH INFORMATION PRIVACY SURVEY (1993).

6. *See* LOUIS HARRIS & ASSOCS. & DR. ALAN F. WESTIN, WORKPLACE HEALTH AND PRIVACY ISSUES (1993).

today, these private-sector employees expressed concern at the same level (seventy-nine percent) that annual Harris surveys found for the general public between 1990 and 1995 (seventy-eight and eighty-two percent).

Several other general findings from the employee survey are significant to note:

- Employees and human resources executives score almost identically in evaluating which types of tests employers should or should not use in deciding whether or not to hire a job applicant. Requiring tests for using nicotine off the job, urine tests for alcohol, and psychological tests are opposed as unacceptably invasive by two thirds or more of both employees and executives, while requiring urine tests for drugs is supported by heavy majorities of both groups.
- Similarly, employees and personnel executives are in close agreement about what information about job applicants should or should not be obtained by employers. Whether educational records are accurate and whether the applicant has ever been convicted of a felony are heavily approved by both groups, while checking on whether the applicant has ever filed a workers' compensation or job discrimination claim are heavily disapproved by both.
- Finally, employees and personnel officials overwhelmingly agree about what kinds of employee off-the-job activities the employer should or should not examine. Over eighty percent of each group agree that employers should not—in pursuit of better employee health and reduced health-benefit costs—forbid employees to engage in dangerous sports or hobbies, drink alcoholic beverages, or smoke tobacco products off the job.

With this profile of how private-sector employees approach workplace privacy issues in general, let me turn to the case study I want to explore for this presentation — employer monitoring of work — and the interplay of values, public and employee opinion, and legal rules.

Privacy and Work Monitoring

Workplaces as Public Sites

Historically, American employers were entitled to see all, hear all, and collect all the information they wished about their employees. Even in today's setting of socially and legally mediated employment

relationships, most of what employees do is still subject to employer oversight.[7]

The general sense of both employees and the public is that employees who enter an employer's premises to do paid work have left "private" space and entered a "public" arena. Employees expect supervisors to observe them coming and going on the premises, as well as to oversee work processes and measure the quantity and quality of work products. Employers regularly collect and use job-relevant information for personnel administration. Also, employers are expected to provide security for persons and property at the work site in order to detect and prevent criminal activity.

At the same time, the U.S. Supreme Court has held for government employment and some statutes have legislated for all employers that employees do have some privacy rights while at the workplace. These arise where there is a "reasonable expectation of privacy" for certain employee activities, even if they take place on the employer's premises—such as using bathrooms, keeping papers in desks or lockers, using a telephone for personal calls, or engaging in legally-protected union organizing at work.[8]

Even here, however, law does not treat such on-premise employee privacy rights as absolute. Corporate security officers can use properly-limited camera and microphone surveillance of bathrooms to obtain evidence of crimes being carried out there. Employers can also search desks and lockers or monitor employee use of the company telephone system for similar investigative purposes.[9] Voice mail and e-mail can also be lawfully monitored by employers because both are business tools that are not provided for personal use and enjoy no immunity from business-related oversight.[10]

However, if employees can show that the real purpose of employer surveillance is not to assure proper work performance or prevent crime at work sites, but to identify whistle blowers,[11] or find out

7. *See* ALAN F. WESTIN, *The World of Work and Personnel Administration*, *in* COMPUTERS, PERSONNEL ADMINISTRATION, AND CITIZEN RIGHTS (U.S. National Bureau of Standards, 1979); Alan F. Westin, *Past and Future in Employment Testing: A Socio-Political Overview*, 1988 U. CHI. LEGAL F. 93.

8. *See* National Labor Relations Act §§7, 8(a)(1), (3), 29 U.S.C. §§ 157, 158(a)(1), (3) (1994) (protection of union organizing activity); O'Connor v. Ortega, 480 U.S. 709 (1987) (privacy of government worker's office, desk, and files); Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (action based on violation of Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2511, 2520 (1994), relating to privacy of telephone conversations).

9. *See Ortega*, 480 U.S. at 725-26.

10. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (discussing e-mail).

11. *See* Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16-35 (1989).

what employees think of management policies, or spy on union organizing campaigns,[12] or satisfy voyeuristic impulses, then American law provides employees with remedies against such improperly-motivated employer behavior.

Monitoring Work Performance

American employers have traditionally been entitled to watch employees when they are actually at work, to supervise their work processes, and to inspect and evaluate their work product according to work standards and procedures set by the employer. Labor unions have long protested when they saw coercive work monitoring used to drive workers to unrealistic and high-stress quotas. These protests have usually focused on unfair standards or inadequate compensation, not on the *fact* of supervisors watching or listening to workers at work. However, wholesale union opposition to work monitoring sometimes functions as an emotionally-charged weapon in the on-going power struggle between management and unions.

The spread of office computerization has brought the work monitoring issue into high prominence.[13] With the proliferation of computer workstations and computerized telecommunication systems in the 1980s and 1990s, employers are now able, through software applications, to generate records of when each employee was at work (or had taken a bathroom break) and how many keystrokes were made at an employee's workstation per minute, hour, day, or week. As for employees doing customer service work on the telephone, the new systems enable employers not only to listen in on the calls (a capacity as old as the telephone itself), but also to compile comprehensive records of how many calls each operator completed and the length of time each call took. Work monitoring systems also allow supervisors to view on a monitoring screen exactly what the employee sees on his or her Video Display Terminal during a telephone call using a customer record, and to watch the employee work on that record.

Since these new monitoring capacities match the classic supervisory techniques of counting widgets produced or letters typed by an

12. *See* NLRB v. Transportation Management Corp., 462 U.S. 393, 395 (1983) (a discharge is discriminatory under the National Labor Relations Act if "an antiunion animus contributed to the employer's decision to discharge [the] . . . employee."); Danzansky-Goldberg Memorial Chapels, Inc., 264 N.L.R.B. 840 (1982), *order supplanted by* Danzansky-Goldberg Chapels, 272 N.L.R.B. 903 (1994).

13. *See* ALAN F. WESTIN ET AL., THE CHANGING WORKPLACE: A GUIDE TO MANAGING THE PEOPLE, ORGANIZATIONAL AND REGULATORY ASPECTS OF OFFICE TECHNOLOGY (1985).

employee, and checking for errors, many employers have adopted electronic monitoring as a regular part of supervision and quality control. Good employers have generally used these techniques sensibly and fairly, and exploitive employers have—predictably—abused them, adding the term "electronic sweatshops" to our computer-age vocabulary.[14]

This brought the issue of electronic monitoring squarely into management-union and employee relations debates in the 1980s and 1990s. Are an employer's work standards fair or oppressive? Do supervisors drive for quantity over quality work, draining jobs of all employee pride and satisfaction? Is monitoring used manipulatively to punish union activists, dissenters, or whistle blowers? Does "oppressive" monitoring lead to harmful stress and increased physical and psychological ailments? Is monitoring conducted in a way that robs employees of basic dignity?

All these are real and important employee and labor relations issues, and the more they are seriously debated and good practices insisted upon by our society, the better. But some union leaders and their supporters decided that there was also a *privacy* issue here. Employers should not be allowed to "eavesdrop" on the conversations between workers and consumers, it was argued, and a broad campaign was launched to outlaw "electronic invasions of employee and customer privacy."

How valid is this privacy-based argument? Not very, since it lacks public support, threatens central societal interests in quality work, and fundamentally misapplies privacy concepts.

Public Support for Fair Employer Monitoring

When some pollsters have asked the public whether it is all right for employers to "listen-in on the telephone calls of their employees," the reactions are thoroughly predictable—the public says no. The question conjures up images of Big Brother employers pruriently eavesdropping on personal calls, prying into attitudes toward management, or searching for "disloyal" workers.

However, a 1994 Louis Harris and Associates survey for Privacy & American Business[15] shows that the public feels (and responds)

14. *See* BARBARA GARSON, THE ELECTRONIC SWEATSHOP: HOW COMPUTERS ARE TRANSFORMING THE OFFICE OF THE FUTURE INTO THE FACTORY OF THE PAST (1988).

15. In March 1994, a series of questions about monitoring were asked on a Louis Harris & Associates survey of 1,255 representative respondents 18 years of age and older. Within this national sample, Harris identified respondents employed full or part time (65%), and, of those,

very differently when asked about employers listening-in on the customer phone calls that employees were hired to conduct, and when the listening-in is done to assure the courtesy and correctness vital to delivering good customer service.

The Harris survey first gave a description of customer service telephone work. "Most companies that employ telephone operators to take customer orders or provide customer service have supervisors who listen-in on the operators occasionally, to see if they are courteous and efficient, and that they follow legal rules as to consumer protection." Then the survey posed two alternative views of such listening-in: "Some groups see this as an invasion of employee and customer privacy, and think all listening-in should be banned. Employers say these are business not personal calls, and that listening-in is necessary to insure proper service to the public. Whom do you tend to agree with?"

Fifty-nine percent of the public (and sixty percent of employed persons) said "listening-in should be allowed." Thirty-nine percent of the public (and thirty-eight perecnt of employed persons) felt it "should be banned." Fifty percent of union members felt listening-in should be allowed, compared to forty-nine percent who would ban it.

Despite a flood of anti-monitoring and "invasion of employee privacy" articles and programs broadcast over the past two to three years, the public continues to find such monitoring reasonable. The fifty-nine percent of the public that now approves occasional listening-in on customer service operators is staying at the same level as the fifty-eight percent who favored monitoring when this identical question was asked in a 1990 Harris privacy survey.

A second question probed the kind of notice to the employee that the public considers appropriate. This asked: "Companies that use listening-in on business calls notify all employees handling business calls that this will be done from time to time. Some groups say that the employee should be personally told in advance *each time* a supervisor will be listening. Employers say this would only put employees on special behavior for those calls, and would not help assure good customer and public service overall. Which position do you agree with?"

Sixty-eight percent of the public (and seventy percent of employees) said that "general notice is sufficient." Twenty-eight percent of

employees represented by labor unions (15%). Standard demographics were collected—age, education, income, sex, race, region, type of community, party identification, and political philosophy.

the public and of employees felt "operators should be notified each time." In an interesting finding, *fifty-nine percent of union members* also felt general notice was sufficient!

Demographically, a majority of Blacks, Hispanics, Democrats, and liberals—groups who usually strongly support privacy in consumer and employment settings—joined union members in saying that notice each time is not necessary. In fact, every demographic group except respondents with less than a high school education supported a general notice policy.

These first two questions on the Harris survey mapped public and group views without any specification of *how* employers would conduct listening-in and what kinds of employee-relations policies would be applied. To see what employer policies the public and employees consider essential to fair monitoring, the survey went on to describe "some policies that employers might use for listening-in on business calls," and asked respondents: "For each, indicate whether you see that policy as necessary for what you consider fair listening-in practices, or not necessary."

The employer policies list presented was drawn from fair monitoring practices recommendations developed over the past decade by experts, employee-relations professionals, and privacy specialists. They are also the key provisions of the Financial Services Industry's Fair Employee Monitoring guidelines, developed in the early 1990s.

By very large majorities—in the seventy-three to eighty-nine percent ranges—the public, employees, and union members all consider the following necessary for fair employer practices:

Employer Practice	Public	Employees	Union Members
"Procedures for listening-in and standards used to evaluate employee call-handling should be fully explained to employees"	89%	93%	92%
"Employees should be told when they are hired for these jobs that supervisors will sometimes listen-in on business calls, so that employees can agree or not agree to work under these procedures"	88%	92%	95%
"Employees whose performance is criticized should have access to any notes or recordings made of their calls, and the opportunity to challenge the supervisor's evaluation"	86%	90%	96%
"Problems with employee performance found from listening-in should lead to additional employee training, and only when performance fails to improve should disciplinary action be taken"	82%	87%	90%
"Listening-in should be done only on business calls, with separate and un-monitored telephone facilities for employees to make personal calls"	73%	78%	83%
"Management should involve employees in setting up the standards and procedures for listening-in on business calls"	73%	77%	84%

Each of these six policies is seen as "necessary" for "fair listening-in practices" by strong majorities of *every demographic group*—all ages; men and women; Black, White, and Hispanic; across the educational spectrum; at all income levels; by Republicans, Democrats, and Independents; among liberals, moderates, and conservatives; North, South, Midwest, and West; and in cities, suburbs, and rural areas.

These findings are striking because people currently employed are more favorable to employers being allowed to monitor customer service calls, in supporting general notice as sufficient, and in favoring the six elements of fair monitoring practices than are respondents not currently employed. This suggests that the work force in daily contact with the nation's private and public employers and those with more actual knowledge of how employer monitoring is being used today do not see monitoring of customer service work as a "privacy" issue at

all. If they did see it that way, given all the Harris survey findings on strong public and employee concerns about privacy invasions, it is clear that employees would favor a ban on listening-in.

Policy Implications from the Survey Results

What the survey findings show is that majorities of the public and of working people are unconvinced that employee privacy is threatened by legitimate employer monitoring of work. It simply offends reason and common sense to assert an immunity from supervision—as a "privacy right"—for business calls. These are, after all, calls handled by the employee, on the employer's line and equipment, when customers call or are being called for the employer's business. Furthermore, poor performance or errors by employees drive away customers, and serious legal liabilities can arise for violating laws on improper telephone offers or promises.

As noted earlier, there are important issues relating to fair standards of work performance, due process rights in the collection and use of performance statistics for discipline or discharge purposes, and the harmful effects on stress levels and mental health if monitoring is oppressive. But when advocates claim that performance monitoring is a privacy issue—and seek state or federal legislation or court rulings to outlaw employer monitoring or provide notice each time monitoring is used—the concept of privacy is stretched beyond its rational limits.

Indeed, pressing for extreme and unfounded privacy claims of this kind could easily lead many policy-makers and the public to conclude that the "privacy movement" in the United States has become so unrealistic and imperial in its claims that the pendulum needs to swing back to much broader support for disclosure and surveillance, not just in employment but on many other organizational fronts as well.

CONCLUSIONS

Unlike the European nations, where detailed codes of data protection for employment (and all other sectors of personal data collection by organizations) are laid down by statute and administered by regulatory data protection commissions, the U.S. approach to privacy remains a more eclectic blend of constitutional interpretation, pinpointed and sector-specific legislation, sector-based administrative agency rules, common-law judicial interpretation, labor-management

bargaining (where employees are union-represented), voluntary organizational policies, and market-based dynamics.

In some sectors—such as protection of privacy for medical records and in health care—I strongly support enactment of pre-emptive federal health privacy legislation. This is because there are systemic abuses and problems in the way individual health records are circulating today well beyond the provider settings; because existing state laws and the common law are too fragmented to serve as road guides in an era of computerizing medical records and electronic health information exchanges; and because both the health care industry and the American public strongly support—and are calling for—enforceable national health privacy rules.

I do not see employee privacy as anything like that situation. On the whole, what we have written into law and judicial decision, and what has not been put into law in the various areas of workplace privacy, is a solid, workable system that strikes the right balances between privacy and other social interests.