UIC Law Review

Volume 23 | Issue 4 Article 4

Summer 1990

Privacy: The Workplace Issue of the '90s, 23 J. Marshall L. Rev. 591 (1990)

David F. Linowes

Ray C. Spencer

PRIVACY: THE WORKPLACE ISSUE OF THE '90s

DAVID F. LINOWES*
RAY C. SPENCER**

I. INTRODUCTION

Many keen observers of employer-employee relations hold that privacy is becoming the workplace issue of the 1990s as the courts, Congress, and state legislatures define employee rights.[1] Workplace litigation is already a major concern for employers as new laws and court decisions expand employers' social obligations to their employees.[2] As medical screening moves beyond drug abuse to genetic and AIDS testing, there is an increase in the number of court cases weighing the employer's right to know against employee expectations of privacy.[3]

Employees bringing suits against their employers is a relatively recent phenomenon. In 1979, there were only a few claims and no jury trials concerning employee privacy.[4] Today, however, there has been a dramatic upsurge in privacy litigation, with juries awarding higher levels of verdicts than ever before.[5]

---

* Professor of Political Economy and Public Policy, College of Liberal Arts and Sciences; Boeschenstein Professor Emeritus; Senior Advisor, Institute of Government and Public Affairs, University of Illinois; David F. Linowes is the former Chairman of the U.S. Privacy Protection Commission.

** Visiting Research Associate, Ph.D., University of Illinois.

1. Bacon, *See You in Court: Employee Suits Against Employers are Turning the Workplace into a Legal Combat Zone*, NATION'S BUS., July 1989, at 17, 26.

2. *Id.* Increased federal and state legislation has expanded employers' obligations to employees giving rise to workplace litigation in suits for wrongful discharge, discrimination, and invasion of privacy. *Id.* at 18-26. *See also* Kleiman, *Worker Privacy Right Puts Businesses to Test*, Chicago Tribune, July 23, 1989, § 8, at 1 (the struggle between employers' need to collect information on their employees and the employees' right to privacy); Goode, *Privacy Rights Now Aired in Public*, INSIGHT, Feb. 1, 1988, at 52 (courts' use of balancing test, weighing the employer's need to know against the employee's right to privacy in the workplace, on the rise).

3. Chapman, *The Ruckus over Medical Testing*, FORTUNE, Aug. 19, 1985, at 57, 60. *Cf.* LOUIS HARRIS & ASSOCIATES, INC., THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE 42 (1990). In this 1989 Louis Harris poll of corporate human resources executives, 3% of the respondents reported invasion of privacy lawsuits being brought against their companies by employees, and 2% said privacy suits had been brought against their firms by job applicants.

4. Bacon, *supra* note 1, at 24.

5. *Id.*

Since 1980, wrongful-discharge court cases have increased dramatically, with courts ruling that employers have an obligation to deal fairly and in good faith with their employees.[6] The employment-at-will theory is rapidly being replaced by a "covenant of good faith and fair dealing" in workplace hiring and firing.[7] Wrongful-discharge claims by ex-employees are often based on the common-law tort of privacy invasion.[8]

A RAND Corporation study found that during one 10-month period from October 1986 to July 1987 there were only 15 total cases reported nationwide that were brought to trial based on the employment-at-will doctrine.[9] During this same period, however, 150 cases based on the covenant of good faith and fair dealing were brought to trial.[10] Although the study concluded that the total number of wrongful-termination suits was still small (only 8.8 trials per million employees nationwide), the number and associated costs to business of employee lawsuits was expected to continue to increase.[11]

To minimize bad hiring decisions and subsequent negligent-hiring lawsuits, employers are using a variety of methods to scrutinize the backgrounds of job-seekers. The Adolph Coors Company, for instance, rejects 50 to 60 percent of its job applicants through a three-step evaluation process.[12] The company uses urinalysis for drug screening, a written "honesty" or integrity test, and a background check performed by an outside firm to screen its new hires.[13] Coors' hiring procedures are representative of those in use throughout corporate America.[14]

Drake University law professor Stanley Ingber warns of a societal trend toward weakening the individual's right to privacy.[15] This trend extends to the workplace where the surveillance of employees is increasingly being perceived as being outside the realm of reasonable privacy expectations. Employers can justify the monitoring of workers if employees are informed of surveillance policies. In many cases, employees must sign privacy waivers as a condition of employment.[16] This weakening of the right of privacy may make additional legal protections necessary.

---

6. *Id.* at 18.
7. *Id.*
8. J. DERTOUZOS, E. HOLLAND, AND P. EBENER, THE LEGAL AND ECONOMIC CONSEQUENCES OF WRONGFUL TERMINATION v, vi (1988).
9. *Id.* at 17.
10. *Id.*
11. *Id.*
12. Nye, *Son of the Polygraph*, ACROSS THE BOARD, June 1989, at 21-22.
13. *Id.*
14. *Id.*
15. Sanders, *Reach Out and Tape Someone*, TIME,.Jan. 8, 1990, at 55.
16. Nye, *supra* note 12, at 21.

Traditionally, the legal system has given employees little protection from privacy invasions on the job.[17] To win an invasion of privacy suit, employees must prove that their reasonable expectations of privacy outweigh the employer's reasons for spying.[18] Employers are generally viewed as having a right to monitor their workers.[19] Further, the employer usually owns the telephone system as well as the premises where the work takes place.[20] Therefore, federal law has given managers the right to monitor employee telephone calls and place video cameras in the workplace.[21]

II. FORTUNE 500 SURVEY

A comprehensive survey we recently conducted at the University of Illinois determined the extent to which the largest industrial corporations of America have policies safeguarding the personal information they collect and maintain about their employees, former employees, and job applicants.[22] A sample of 275 companies was selected from among the Fortune 500 corporations. One hundred twenty-six companies, or 465 firms representing over 3.7 million employees, responded. Because major corporations are standard setters of business practices, the impact of the policies described goes well beyond the Fortune 500 corporations.

A. Disclosures of Personal Employment Data

Four out of five companies (80%) disclose personal information to credit grantors and 3 out of 5 (58%) give information to landlords. One fourth (28%) gives it to charitable organizations. Yet, most companies (57%) do not tell the individual about it.

For inquiries from government agencies, 2 out of 5 companies (38%) do not have a policy concerning which personal records are disclosed. When no policies exist, a computer technician, file clerk, or any of a number of other individuals handling the records decides what personal information is turned over to the government, whether the agency is entitled to it or not.

---

17. Weingarten, *Communications Technology: New Challenges to Privacy*, 21 J. MARSHALL L. REV. 735, 746 (1988).

18. Rothfeder & Galen, *Is Your Boss Spying on You?*, BUS. WEEK, Jan 15, 1990, at 74-75.

19. Weingarten, *supra* note 17, at 746.

20. *Id.*

21. *Id.*

22. The following statistical information was originally reported in D. LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? 40-61 (1989) [hereinafter PRIVACY IN AMERICA].

B. Individual Access

While most corporations (87%) give employees access to their personnel records, only about one in four (27%) allows access to supervisors' records. Four out of five corporations (77%) allow employees to place corrections in their personnel records, and nine in ten (87%) forward these corrections to anyone who received the incorrect information.

C. Informing the Individual

Four out of ten corporations inform personnel of the types of records maintained (43%), how they are used (41%), and what company disclosure practices are (42%). Two of five (42%) of the corporations responding find it necessary to collect information without informing the individual. Four out of five organizations (78%) check, verify, or supplement background information collected directly from personnel.

Over half of the companies do not tell their employees the types of records they maintain (57%) or how they are used (59%). These companies, in effect, are maintaining secret records, which is anathema to a democratic society. Although 4 out of 5 (78%) verify or supplement background information collected from their personnel, less than one half (44%) let the individual see the information.

D. Authorizing Personal Data Collection

One out of three companies (34%) seeks information from a third party without written permission. When written permission is not obtained, most corporations do not have a policy of informing an individual of the types of information sought (71%), the techniques used to collect it (80%), or the sources consulted (75%).

E. Medical Records

Half of the companies use medical records about personnel in making employment-related decisions. One in five (19%) does not inform the employee of such use.

Two out of three (65%) of the companies responding have restrictions in regard to smoking, but in all cases such restrictions apply to places where smoking is allowed. One of fifty companies (2%) shows in its personnel records whether an employee is a smoker or non-smoker.

F. Drug Testing

Over half (58%) of the corporations have a drug-testing program in operation. Nine out of ten (89%) use the program for pre-employment screening. One quarter (22%) of the companies responding have a drug policy, but no testing program. Nine out of ten (86%) had a drug-testing program for two years or less. Nearly all (97%) began the program because of general concern for the safety of employees. None of the companies release the results of drug tests to outside organizations.

G. AIDS Testing

Three percent have an AIDS-testing program in operation, and it has been in operation for less than a year. None of the companies release results to outside organizations. Another five percent have an AIDS-testing policy, but no testing program. Ninety-two percent have neither a policy nor a testing program, and it is not likely that they will institute an AIDS-testing program in the next two years. Yet, two of five companies (42%) believe that government, as opposed to business, should conduct more stringent AIDS testing in screening personnel.

H. Polygraph Use

Eighty-five percent of the companies did not use the polygraph or other truth-verification equipment even prior to December, 1988, when the federal law prohibiting the use of polygraphs in pre-employment screening went into effect. Practically all (95%) of the 15% that did use such equipment did so under circumstances of possible theft or shortage. One in three (32%) of the companies responding believed more stringent polygraph testing policies should be used by the government as opposed to business. The main reasons most companies did not use polygraph testing were validity and reliability of the tests (43%) and moral or ethical implications of use (34%).

I. Use of Investigative Firms

Over half (57%) of the organizations responding retain the services of an investigative firm to collect or verify information concerning personnel. About one in five (19%) of these corporations does not review the operating policies and practices of the investigative firm.

J. Arrest and Conviction Records

Ninety-one percent of the companies do not require the collection of arrest records of personnel. Three out of five (57%) do not require information on convictions.

K. General Practices

Over half of the companies (55%) have a policy for conducting periodic evaluations of their personnel record-keeping systems, and within the past two years, nearly half (49%) of the respondents conducted a systematic evaluation of their existing personnel record-keeping practices with particular attention to confidentiality safeguards. Almost three out of four companies (72%) have designated an executive-level person to be responsible for maintaining privacy safeguards in employment record-keeping practices. Practically all (98%) of the companies utilize computer facilities for record keeping, and 97% of payroll records information, 94% of personnel records, and 56% of group insurance records are in a common data bank. No employment applications inquire about an applicant's sexual preference.

L. Summary of Results

The policies and methods used by an employer to manage the personal information files of employees can have a significant impact on the lives of those employees. Often, information of a personal nature is collected and included along with pertinent personnel data. Even medical information and sometimes the results of drug testing are included. Employees are, in many instances, denied access to all or portions of their own files while the employer may release the same information to third parties. Employees who are allowed access to files may not be allowed to correct errors.

M. Implications

Business decisions, such as hiring and promotion, are sometimes made on the basis of information that should never have been included in the file. A totally unsubstantiated negative item can result in a tarnished career. Release of this kind of information to third parties could compound the damage.[23]

For example, in one case the time had arrived when John, the executive vice-president who had devoted his twenty-year career to the company, expected to be appointed president. The incumbent

23. *Id.* at 27.

president was retiring in four months and a committee of the board of directors had been designated to formally make the recommendation for his successor. To the shock of John and his colleagues, when the announcement was officially made, the selection turned out to be the second vice-president, a man with far fewer credentials and less time with the company.

All explanations by the board spokesperson rang hollow, and John was determined to get the full story. He hired a lawyer who subpoenaed the files of the selection committee. Those files revealed a complete copy of his medical records maintained by his personal physician. In his physician's scrawled handwriting was the notation, "patient seems to have trouble managing his finances." The notation was made at a time when John was having persistent headaches and his doctor was probing all possible causes, including mental pressures.

The selection committee of the board of directors of the company, studying that notation, reasoned that if the executive vice-president could not manage his own finances, they could not risk recommending him for the presidency where he would have to manage the finances of the company. If John had not insisted on learning the full facts and backed that insistence with expenditures for legal counsel, he never would have learned that the casual notation by the physician contributed to the devastating result. Although too late to prevent the harm already done, now at least he was able to explain and correct the record to avoid additional damage.

III. Threats to Employee Privacy

A. Historical Context

Workplace privacy threats are not a new phenomenon. In the early part of the twentieth century, for instance, privacy safeguards for employees were almost nonexistent. At that time, the Ford Motor Company had a sociological department with one hundred investigators who would go into the workers' homes to make sure that no one was drinking too much, that their sex lives were unblemished, that houses were clean, and that leisure time was spent profitably.[24] Workers found wanting were fired from their jobs which paid $5.00 a day.[25] Employment applications in those days asked prospective employees to name their political leader, and if they smoked, gambled,

24. *Id.* at 31. *See also Body Invaders*, The Nation, Jan. 8, 1990, at 40 (Department of Transportation extends routine drug testing program to four million private industry employees; an old scam with a new look).

25. Privacy in America, *supra* note 22.

swore, used slang, or had ever been divorced.[26]

At the turn of the century, the personnel policies of private business may have been intrusive, but information collected on workers was generally used only by the particular employer.[27] There were no computer data banks to store knowledge indefinitely, and personal files could not be instantly retrieved or transmitted around the world.[28] In today's society, problems concerning employee privacy are compounded due to the widespread use of technology.

B. The Menace of Technology

Firms engaged in employee monitoring, including drug testing, AIDS testing, genetic screening to identify genes linked to illnesses, polygraph tests, voice stress analyzers, and psychological tests, now have a number of high-tech tools available to assist them.[29] According to Professor David H. Flaherty of the University of Western Ontario, increased automation and the proliferation of databanks have led to the insidious electronic monitoring of workers.[30] Adding to the problem, Flaherty says, is the ability of new technology to outpace existing regulations leaving employees to rely on the self-regulation of their bosses.[31]

Fred Weingarten, Communications and Information Technologies Program Director with the Office of Technology Assessment, has written that innovations in technology are shifting the balance of power between the employer and employee giving employers an unfair advantage.[32] Weingarten suggests companies establish a "broader consensus" for protecting the privacy rights of their workers.[33] He adds that if firms fail to adopt voluntary standards for individual privacy protection, new laws may become necessary.[34]

C. Computerized Records

Increased workplace computerization has enhanced the possibility of threats to individual privacy. Daily work output profiles are prepared on a variety of individuals, including airline reservation clerks and clerical personnel.[35] Employee perceptions of a lack of

---

26. *Id.*
27. *Id.*
28. *Id.*
29. Weingarten, *supra* note 17.
30. D. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 3 (1989).
31. *Id.* at 4.
32. Weingarten, *supra* note 17.
33. *Id.* at 753.
34. *Id.* at 746.
35. D. FLAHERTY, *supra* note 30, at 3. *See also* Conniff, *How Do You Spell Boss? S-P-Y*, NEXT, July/Aug. 1981, at 71 (Computers measure employee output and moni-

control over their own personnel files has led to greater fear of possible privacy violations. A 1989 study of employee perceptions of the security of computerized human resource records showed that employees were more likely to be concerned about which individuals and organizations had access to personnel files than what the records contained.[36] Concerning the content of personnel files, employees said material relating to their jobs, including pay rate, fringe benefits, and educational history, was the most sensitive.[37]

D. Drug Testing

Since the mid-1980s, there has been a significant increase in drug- and alcohol-abuse testing of employees.[38] The primary drug-testing procedure is urinalysis, but drug use can also be detected through blood and hair analysis.[39] According to a 1988 Department of Labor survey, about 60 percent of companies with 5,000 or more employees have drug-testing programs, including IBM, Kodak, and Du Pont.[40] Among businesses with 50-99 employees, 12 percent of the firms reported testing for drug use. Another 15 percent said they were considering implementing tests.[41]

1. Urinalysis

Often, firms require employees to submit to urinalysis as a prerequisite to obtaining or keeping a job. It costs employers between $25 and $100 for the tests,[42] and testing has become a $300 million-a-year industry for businesses producing urinalysis kits and operating diagnostic labs.[43] The practice of testing for drug use is spreading rapidly in an effort to lessen accidents, absenteeism, and low productivity. Employers are beginning to test workers already on the payroll, and some school systems are considering testing both

---

tor employee activity).

36. Taylor & Davis, *Individual Privacy and Computer-Based Human Resource Information Systems*, 8 J. BUS. ETHICS 569 (1989).

37. *Id.*

38. Bacon, *Business Moves Against Drugs*, NATION'S BUS., Nov. 1989, at 82. *See also* Drexler, *The Office Drug Test Craze: Is it a Workplace Safeguard or an Invasion of Privacy*? Atlanta Journal, Feb. 11, 1990, at D1, col. 5 (stretching the bounds of workplace drug testing more trend than cure).

39. *See*, Isikoff, *Splitting Hairs to Find the Roots of Drug Use*, Wash. Post, Mar. 14, 1990, at A15 (use of mass spectrometer to detect drugs in hair samples expands from law enforcement to private industry); *Seeking to Ensnare with a Strand of Hair*, PRIVACY J., Mar. 1988, at 1 (employer finds drug tests on hair samples foolproof and evasion-proof).

40. Bacon, *supra* note 38, at 84.

41. *Id.*

42. *Id.*

43. Morganthau, *A Question of Privacy*, NEWSWEEK, Sept. 29, 1986, at 18.

teachers and students.[44]

A recent survey of over 700 U.S. corporations, government agencies, and organizations, conducted by Executive Knowledgeworks, found that over 200 of the firms had drug-testing programs.[45] The study also found that 16 percent of employees not passing drug tests are subsequently fired.[46] Those using urine tests to check for marijuana or drug use now include police and fire departments, the Ford Motor Company, and the National Football League.[47] Urinalysis is not always accurate, and critics say the drugs detected often have no effect on job performance.[48] In Washington, D.C., a few years ago, city officials had to reinstate 24 of 39 police recruits suspended for the detection of drug use.[49] Unfortunately for the 24 reinstated recruits, the city had already publicly announced them as marijuana users.[50]

A 1986 survey of 497 national companies conducted by the College Placement Council found that nearly 30 percent of employers of new college graduates required drug screening, usually including urinalysis.[51] Almost all of the firms having screening programs tested for both marijuana and hard drugs.[52] Safety was listed as the primary reason for the testing of job applicants, and most firms using the screening reported that they would not hire applicants who failed drug tests.[53]

2. Limitations of the Tests

Some people claim that urinalysis can show whether a person is being treated for a heart condition, epilepsy, diabetes, or asthma, and that such screening can become more of a device for monitoring off-the-job activity than a test for actual job performance.[54] Most of the tests do not determine if drugs are actually used on the job.[55] Often, cocaine can be detected in the urine up to three days after

---

44. Gest, *Using Drugs? You May Not Get Hired*, U.S. NEWS & WORLD REP., Dec. 23, 1985, at 38.

45. PRIVACY IN AMERICA, *supra* note 22, at 36.

46. *Id.*

47. Gest & Scherschel, *Report on Privacy: Who is Watching You?* U.S. NEWS & WORLD REP., Jan. 12, 1982, at 34, 36.

48. *Id.*

49. *Id.* The urine samples had been mishandled. *Id.*

50. *Id.*

51. COLLEGE PLACEMENT COUNCIL, INC., PREEMPLOYMENT DRUG SCREENING: A SURVEY OF PRACTICES AMONG NATIONAL EMPLOYERS OF COLLEGE GRADUATES (1986). The participating employers represent a 41.5 percent response rate. *Id.*

52. *Id.*

53. *Id.*

54. Glass, *Testing: Are You Next?* PUBLIC SERVICE REPORTER, July/Aug. 1987, at 1, 5.

55. Dentzer, *Can You Pass the Job Test?* NEWSWEEK, May 5, 1986, at 46.

consumption.[56] Trace chemicals may be present from five days to three weeks after marijuana is used.[57] Over-the-counter drugs containing ibuprofen, such as Advil® and Nuprin®, have shown up as illegal substances in some tests.[58] False accusations of marijuana abuse may also result from fragments of the skin pigment melanin that can be detected in the urine.[59] Melanin, which is present in everyone but is usually at higher levels among blacks and Hispanics, can break down and produce positive results in urinalysis testing even for people who have never used marijuana.[60]

Critics of drug testing say its costs may not be justifiable for widespread use. The U.S. military spends about $100 for the collection, transportation, analysis, and reporting of each test in its urinalysis program.[61] If every employee in the U.S. work force were to be tested in a similar manner, the cost to society would be $8 to $10 billion per year.[62]

3. *Examples of Testing Abuse*

Drug-testing programs often lead to the abuse of workers' rights. In one case, an employee was accused of being a narcotics user by his supervisors after his drug test revealed traces of methadone.[63] Although a follow-up test later showed the substance was actually a normally occurring compound which resembled methadone, the man was fired on the pretext of failing to report an on-the-job accident in a timely manner.[64] The man then sued his former employer, claiming that his rights had been violated.[65] The court held that the employer had made false statements about the man's use of drugs and that the employee was entitled to punitive damages.[66]

In some cases, drug tests falsely indicate the presence of drugs.[67] These "false-positive" results can have devastating consequences for the individuals involved. For instance, a California office

---

56. *Id.*
57. *Id.*
58. *Id. See also* Morganthau, *supra* note 43 (numerous legal drugs produce "false positive" and "false negative" results when urinalysis is conducted carelessly).
59. Dentzer, *supra* note 55.
60. *Id.*
61. Lundberg, *Mandatory Unindicated Urine Drug Screening: Still Chemical McCarthyism*, 21 J.A.M.A., 3003, 3005 (1986).
62. *Id.*
63. Chineson, *Mandatory Drug Testing: An Invasion of Privacy?* TRIAL, Sept. 1986, at 91, 93.
64. *Id.*
65. *Id.*
66. *Id.*
67. See Chapman, *supra* note 3, and Morganthau, *supra* note 43, for a discussion of "false positive" and "false negative" test results.

manager, who said he had not used drugs except for nonprescription allergy medicine, charged his employer with invasion of privacy and unlawful imprisonment claiming he was the victim of a false-positive drug test.[68] After the man had failed a urinalysis test, he was told that he would have to participate in drug rehabilitation even if a follow-up test proved negative.[69] The second test was negative and the employee was forced to attend a 28-day, in-hospital treatment program along with Narcotics Anonymous meetings twice a week, and submit to further random drug tests.[70] He consented to his employer's demands to keep his job, but after undergoing at least ten more drug tests, he filed a lawsuit.[71] The court held that the employer could not force the man to attend the treatment sessions and could not subject him to continued drug testing.[72]

Although most company drug-testing programs choose workers at random for the tests, many firms have installed special drug abuse "hot lines" that employees can use to report fellow workers suspected of using drugs on the job.[73] Two employees of a nuclear power facility who had reported safety abuses at the plant to the Nuclear Regulatory Commission (NRC) claimed they were wrongfully terminated because they had been whistleblowers.[74] They believed their employer used a fabricated hot line call to force them to submit to urinalysis.[75]

One of the employees said she had been unable to complete the drug test after being forced by a company nurse to drop her pants to her ankles, bend over at the waist and hold a specimen bottle between her legs with one hand while holding the other hand in the air.[76] After wetting herself, the woman refused to try again and was subsequently fired for insubordination.[77] The second employee's test revealed traces of marijuana, but she was fired for misconduct.[78] Had she been terminated for drug use, the plant would have been forced by the NRC to undertake an expensive check of the woman's work as a quality controller.[79]

---

68. Chineson, *supra* note 63.
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.* at 93-94.
73. Weiss, *Watch Out: Urine Trouble*, HARPER'S, June 1986, at 56.
74. *Id.*
75. *Id.* at 57.
76. *Id.* The Syva Company developed the test administered to the Georgia Power employees aided, in part, by federal funding. The cost of the test is 1/10th of the cost of more precise laboratory procedures. Results are ready in ninety seconds, but give false positive readings in approximately 33 percent of tests.
77. *Id.*
78. *Id.*
79. *Id.*

4. Court Decisions on Drug Testing

In 1989, the Supreme Court determined that personal privacy rights should be abbreviated in regulated industries when failure to eradicate on-the-job drug use could have disastrous effects. In *Skinner v. Railway Labor Executives' Ass'n.*,[80] Department of Transportation safety regulations calling for breath, blood, and urine drug testing of all employees were upheld by the court.[81] In another case, *National Treasury Employees Union v. Von Raab*,[82] the court ruled that a customs service employee drug screening program was constitutional. The program requires testing of employees taking positions directly involved in drug interdiction, the carrying of firearms, or having access to classified information.[83]

The government also requires federal contractors to operate a "drug-free workplace." Under the Drug-Free Workplace Act of 1988,[84] contractors must certify that their work environment is drug free. Although the act does not require drug testing and does not pertain to off-the-job activities, it directs employers to establish drug-alert awareness programs and make employees aware of drug counseling opportunities.[85]

E. Undercover Surveillance

A few years ago, General Motors, the nation's largest private employer, decided to hire undercover agents from a private detective firm to work on assembly lines in its plants to combat drug and alcohol abuse problems.[86] The company estimates that such abuses involve at least one out of every ten workers.[87] While the sting operation led to the arrest of nearly two hundred people, most of whom were GM employees, union leaders complained that this tactic was unprofessional and unfairly concentrated on union members instead of management.[88]

The use of undercover personnel posing as employees is unregu-

---

80. 109 S. Ct. 1402 (1989).

81. *See generally* Malia, *Drug Testing in Regulated Industries: Public Interest Versus Employee Privacy*, PUB. UTIL. FORT., Apr. 27, 1989, at 48.

82. 109 S. Ct. 1384 (1989).

83. Malia, *supra* note 81, at 48-49.

84. Drug-Free Workplace Act of 1988, 41 U.S.C. § 701 (1988).

85. Malia, *supra* note 81, at 51.

86. Burrough, *Inside Jobs: How GM Began Using Private Eyes in Plants to Fight Drugs, Crime*, Wall St. J., Feb. 27, 1986, at A1, col. 6. *See also* Schwartz, *Using 'Spies to Win a War'*, NEWSWEEK, Nov. 6, 1989, at 56 (corporations supplementing drug education programs and random testing with private investigators to root out drug users and dealers in the workplace).

87. Burrough, *supra* note 86.

88. *Id.*

lated by law.[89] However, a few states prohibit employers from disciplining employees on the basis of an investigator's report, unless a copy of the report is given to the employee or an opportunity is provided for the employee to confront the individual making the allegations.[90]

F. Illegal Searches

An employer's right to search employees or their belongings has not been clearly defined by the courts. Generally, if an employer wants to reserve the right to search lockers or desks, this must be conferred to employees in written company policies.[91] For instance, an employee of the K mart Corporation, whose purse and locker were searched without her consent, sued her employer and was awarded $108,000 in damages.[92] The court held that having supplied her own lock for the locker, the woman had a reasonable expectation of privacy.[93] An emerging problem concerns the information kept on personal computers. Looking through someone's desk might be viewed as an invasion of privacy, but calling up information on a computer screen is often considered acceptable business practice.[94]

G. Genetic Screening

A 1982 survey conducted by the Office of Technology Assessment found that eighteen major U.S. companies had used genetic screening of employees to test for high vulnerability to toxins.[95] Genetic screening is used to identify individuals susceptible to disease caused by dust or fumes in the workplace. One genetic test probes for a gene called HDL (high density lipoprotein).[96] People with high HDL levels are less susceptible to heart attacks.[97] HDL influences the body's ability to remove cholesterol from tissues.[98] Genetic monitoring can also involve periodic checks of employees to determine signs of chromosomal abnormalities, such as those influencing cancer or miscarriage rates among women due to workplace chemicals

---

89. Geidt, *Drug and Alcohol Abuse in the Work Place: Balancing Employer and Employee Rights*, 11 EMPLOYEE REL. L. J. 181, 189 (1985).
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. B. GARSON, THE ELECTRONIC SWEATSHOP: HOW COMPUTERS ARE TRANSFORMING THE OFFICE OF THE FUTURE INTO THE FACTORY OF THE PAST 220-24 (1988).
95. OFFICE OF TECHNOLOGY ASSESSMENT, THE ROLE OF GENETIC TESTING IN THE PREVENTION OF OCCUPATIONAL DISEASE 9 (1983).
96. Patterson, *Genetic Screening: How Much Should We Test Employees?*, INDUSTRY WEEK, June 1, 1987, at 45, 49.
97. *Id.*
98. *Id.*

or radiation exposure.[99]

While employers say the tests lower medical costs and enable workers to avoid hazardous employment, many labor leaders and those concerned with personal privacy see dangers in labeling certain individuals or groups as "high risk." Such labeling could involve a loss of career or health insurance coverage for the worker. Problems extend to a specific race being singled out and denied certain types of employment.[100] Also, employers may face lawsuits for failing to dismiss susceptible employees. While current genetic tests cannot account for the effects of confounding factors such as smoking, drinking, or inherited illness, within two or three years the technology of the screening may advance to the point where such tests could be made mandatory for companies in high-risk industries.[101]

H. Polygraphs

Recognizing the polygraph's limitations, Congress passed the Employee Polygraph Protection Act of 1988 which prohibits the use of lie detectors by private companies in pre-employment screening and for random testing of employees.[102] Only pharmaceutical companies and private security firms are exempt from the ban, and the administration of any lie detector test must conform to federal guidelines to insure accuracy and fairness.[103]

Many employers claim the polygraph is a necessary tool to help thwart crimes committed by their workers.[104] No reputable citizen would deny the employer's right to aggressively protect company assets and expose employee dishonesty. Nor would any informed individual dispute the economic reality that employee theft boosts the selling price of merchandise. On the other hand, the arguments against polygraphs concern the ways they are used, their margin for error, and the unfair interpretations that may result from the findings.[105]

In administering polygraph tests, blood pressure tubes are attached to the subject's arm and chest and electrodes placed on the fingers.[106] Then, the person is asked a series of questions while emo-

---

99. *Id. See also* Nelkin & Taneredi, *Biotechnology: A New Power; A New Danger*, Atlanta Constitution, Feb. 16, 1990, at A15, col. 1 (genetic screening threatens traditional concepts of privacy and personal autonomy).

100. *Id.*

101. See Chapman, *supra* note 3, for a discussion of medical dianostic testing in the workplace.

102. 29 U.S.C. §§ 2001-2009 (1988).

103. 29 U.S.C. §§ 2006-2008 (1988).

104. See P. EKMAN, TELLING LIES 219-23 (1985) for a discussion of polygraph testing in pre-employment situations.

105. *Id.*

106. *Id.* at 114, 197-98.

tional response is registered by pen and ink on a paper roll.[107] Physical changes recorded during the test include alterations in blood pressure, pulse rate, and respiration that may occur when a person lies.[108] A negative result on the test, measured by irregular marks on the paper, may not mean that the subject is guilty.[109] Some people's inherent nervousness causes recordings that resemble those made when lying [110] Others are able to consistently pass such a test even when not telling the truth.[111] The questions asked may be unreasonably intrusive, and the polygraph device itself is not sufficiently reliable.[112] On balance, it is fair to conclude that the use of polygraph testing abuses an employee's privacy rights.

I. Voice-Stress Analyzers

If the polygraph raises citizen concern about privacy invasion, the voice-stress analyzer[113] is even more suspect. Firms that sell the device claim guilt produces stress and the absence of stress is evidence of innocence. The degree of accuracy achieved, however, is debatable. Operators of voice-stress analyzers concede that the device does not work on psychopathic liars.[114] Further, all agree that the test is no more efficient than the operator who administers it.[115]

J. Psychological Tests

Since federal law bans the use of lie detector tests for pre-employment screening, many employers are using written honesty tests.[116] A former Target Stores employee, Sibi Soroka of Lafayette, California, filed suit against the retail chain based on having to take a psychological test as a condition of employment.[117] Over 700 items

---

107. *Id.*
108. *Id.*
109. *Id.* at 199.
110. *Id.*
111. *Id.* at 217.
112. *Id.* at 208, 222-23. *See generally* Greenhouse, *Machines That Try to Read Minds*, N.Y. Times, Jan. 26, 1986, at 4E, col. 3; Williams, *Bar Lie-Detector Use by Private Firms?* U.S. NEWS & WORLD REP., Feb. 3, 1986, at 81 (interview with sponsor of legislation barring use of polygraph by private employers).
113. REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 239 (1977) [hereinafter PRIVACY PROTECTION STUDY]. The device, which uses voice inflections to measure stress, may be used without the subject's knowledge. *Id.*
114. PRIVACY IN AMERICA, *supra* note 22, at 36.
115. *Id.*
116. Harlan, *Written 'Honesty' Tests Draw Interest As Law Bars Polygraphs as Hiring Tool*, Wall St. J., Jan. 3, 1989, at B4, col. 2.
117. Williams, *Suit Challenges Target Stores' Use of Psychological Tests for Hiring*, L.A. Times, Sept. 8, 1989, at 1, col. 4; Chung, *Former Store Detective Sues Chain Over Test*, San Francisco Chron., Sept. 8, 1989, at A6, col. 1.

comprised the Target test. Items that Soroka objected to included:

(1) I feel that there is only one true religion;

(2) I am strongly attracted to members of my own sex;

(3) I believe in the second coming of Christ;

(4) I have no difficulty starting or holding my urine.[118]

Although Soroka passed the test and was hired as a security guard, he said he felt "humiliated" and "embarrassed" by the questions which probed his "innermost beliefs and feelings."[119]

In 1988, 56 percent of employers surveyed by the American Society for Personnel Administration said their use of written pre-employment tests had increased in the last five years.[120] Reasons given for not testing included legal problems (52%), time involved (44%), and cost (33%).[121] Ten percent said they used written honesty tests.[122] Companies publishing the tests say 5,000 to 6,000 firms are now using this method of pre-employment screening.[123]

Written honesty tests are relatively inexpensive. Costs range from $6 to $15 each compared with $25 to $75 for polygraph tests.[124] Written tests are also popular because they can be administered and scored by clerical staff. Proponents of testing say certain types of individuals, such as those likely to steal from their employers, have distinctive test-answer profiles.[125] One retail chain reported a 28 percent drop in employee theft after it began testing new hires.[126] Another group of 30 convenience stores reported employee theft losses dropping from $515 per store to $249 per store after honesty tests were introduced.[127]

K. Electronic Surveillance

The growing number of negligent-hiring court decisions which have held companies liable for workers' crimes or negligence on the job has led to extensive employee surveillance.[128] Computerized electronic devices constantly monitor the nation's offices and factories. Surveillance of workers on assembly lines, in offices, and in stores is

---

118. Williams, *supra* note 117, at 11, col. 3.
119. Rothfeder & Galen, *supra* note 18, at 74.
120. Nye, *supra* note 12, at 21.
121. *Id.* at 23.
122. *Id.* at 21.
123. *Id.*
124. *Id.* at 23.
125. *Id.* The publishers of honesty tests provide their subscribers with test norms that indicate the level of risk involved in hiring applicants with various scores. *Id.*
126. *Id.* at 23.
127. *Id.* at 24.
128. Rothfeder & Galen, *supra* note 18, at 74.

now more intense than ever before. General Electric Company, for example, uses tiny, fish-eye lenses in walls and ceilings to monitor employee activity.[129] The Du Pont Company has hidden, long-distance cameras monitoring its loading docks.[130] Other companies have special chairs that measure excessive "wiggling" of workers.[131]

Productivity and behavior of executives are watched as well. In the much-advertised electronic office, data-processing machines are both work tools and surveillance devices.[132] Many office dictation systems, such as Dictaphone's Mastermind and Lanier's Supervision IV, monitor executives by producing records of the volume and type of work being performed.[133] Secret taping has become one of the most common forms of electronic surveillance in the U.S. today with electronic "bugs" being used to eavesdrop on conversations in offices and boardrooms.[134] The sophisticated monitoring equipment includes attache cases with hidden taping devices that can surreptitiously record 30 hours of conversations from up to 50 feet away.[135]

1. Telephone Monitoring

Telephone systems are now being used which automatically record all office phone calls. Dictaphone's voice-activated Veritrac 9000, for example, can record 240 separate telephone conversations simultaneously.[136] Other machines electronically track and time all calls. The resulting printouts allow managers to monitor employee phone use.[137] According to the Communications Workers of America, a group opposed to workplace surveillance, supervisors monitor an estimated 400 million employee telephone calls each year.[138] Companies that say they monitor employee phone conversations include United Airlines, American Airlines, United Parcel Service, Nynex Corporation, Spiegel, Inc., and *The Wall Street Journal*.[139]

Critics of workplace surveillance say it is counterproductive because it can lead to increased stress, fatigue, and turnover among workers.[140] They also say workers are sometimes unfairly judged for

---

129. *Id.*
130. *Id.*
131. *Id.*
132. B. GARSON, *supra* note 94.
133. *Id.*
134. *See generally* Abramson, *Mind What You Say; They're Listening*, Wall St. J., Oct. 25, 1989, at B1, col. 3.
135. Byron, *In Tapes We Trust*, NEW YORK, Oct. 23, 1989, at 40-41.
136. *Id.*
137. B. GARSON, *supra* note 94, at 221-22.
138. Abramson, *supra* note 134.
139. *Id.*
140. English, *Is Your Friendly Computer Rating You on the Job?*, U.S. NEWS & WORLD REP., Feb. 18, 1985, at 66.

falling below predetermined, arbitrary goals set with the aid of computer monitoring.[141] For example, it was reported in the press that Maevon Garrett of Baltimore, Maryland, who had spent eighteen years with AT&T, felt she was unfairly fired in 1984 from her job when the computer revealed she took an average of thirty seconds per caller.[142] She was reinstated after a protest by the Communications Workers of America.[143]

Last year, it was revealed that the Connecticut state police had bugged incoming and outgoing calls at its headquarters, and similar, unauthorized phone taping was discovered at police departments in Rhode Island, West Virginia, and Utah.[144] Many companies that take phone orders from customers, such as Wall Street brokerage firms, are taping the conversations their employees have with clients.[145] The tapes provide a way of settling disputes that may arise in the course of business, but those involved often do not know they are being monitored.[146] Investment companies that acknowledge taping include Merrill Lynch, Kidder, Peabody, Prudential-Bache, Morgan Stanley, Bear Stearns, and Shearson Lehman Hutton.[147]

Federal statutes allow the taping of conversations if at least one of the parties knows of the recording.[148] Although 83 percent of the respondents in a 1978 Louis Harris poll said employers should be forbidden by law from listening in on the conversations of employees,[149] only four states—California, Illinois, Pennsylvania, and Florida—have made one-party-consent recording illegal.[150]

2. *Caller-ID*

Currently, some of the nation's largest corporations, including American Express and J.C. Penney, are taking advantage of new caller identification technology that automatically records callers' telephone numbers.[151] At J.C. Penney catalog offices, for instance, callers are immediately identified by phone number and their de-

---

141. *Id.* Legislation has been introduced in the House and Senate — H.R. 2168, 101st Cong., 2d Sess. (1990) and S. 2164 101st Cong., 2d Sess. (1989), respectively — that would prevent potential abuses of electronic monitoring of employees in the workplace.

142. *Id.*

143. *Id.*

144. Rothfeder & Galen, *supra* note 18, at 75.

145. Byron, *supra* note 135.

146. *Id.*

147. *Id.*

148. *Id.*

149. LOUIS HARRIS & ASSOCIATES, INC., THE DIMENSIONS OF PRIVACY 35 (1979)

150. Byron, *supra* note 135.

151. Carnevale & Lopez, *Making a Phone Call Might Mean Telling the World About You*, Wall St. J., Nov. 28, 1989, at A1, col 1.

tailed account information appears on a computer screen.[152] *USA Today* logs the phone numbers of individuals dialing its national weather hot line for use in later promotions.[153] Although there are beneficial business applications of this technology, there is also potential for privacy abuse.[154]

3. Computer Monitoring

Employers are not only bugging and taping their employees, they are monitoring them through computer terminals. Seven million workers nationwide are linked to computers through video display terminals, and one-third of them are believed to be monitored by computer.[155] Delta Airlines uses computers to track which employees make the most reservations.[156] Safeway Stores, Inc., of Oakland, California, has on-board computers in 782 trucks that monitor driving speed and how long trucks are stopped.[157] Safeway uses the computer reports to suspend or discharge up to 20 drivers a year.[158]

Computer monitoring is being used in some businesses to keep track of employees second-by-second as they work.[159] Anyone touching a keyboard can be monitored. Monitoring the speed and efficiency of employees with computers is beginning to supplement and even replace surveillance with video cameras. Computers track such things as the number of keystrokes per hour for typists, or the amount of time telephone operators spend on the phone with each caller.[160] Increasingly, workers must inform the computer when they go to the restroom.[161] Through magnetized identification cards, employees are automatically checked in and out as they go from one location to another, and an electronic record is made of their movements.[162]

Employee surveillance remains essentially an uncharted legal area. Some observers say this new employee snooping technology has already created "electronic sweatshops."[163] Administrators claim the purpose of the monitoring is to improve employee supervision

152. *Id.*
153. *Id.*
154. *Id.* Businesses purchase computerized phone listings from long-distance companies of customers placing calls to 800 and 900 numbers. *Id.* The listings are then fed into the purchaser's computers and matched with other data. *Id.*
155. English, *supra* note 140.
156. Rothfeder & Galen, *supra* note 18, at 74.
157. *Id.*
158. *Id.* at 74-75.
159. English, *supra* note 140.
160. Id.
161. B. GARSON, *supra* note 94, at 122.
162. *Id.*
163. Furchgott, *Management's High-Tech Challenge*, 2 EDITORIAL RES. REP. 484 (1988).

and to help determine who is eligible for promotion or salary increases.[164] The installation of monitoring systems without restraining controls, however, enables supervisors and co-workers to snoop at will into employees' work lives.

L. Background Checks

Courts in many states now hold employers liable for the conduct of their employees in negligent-hiring cases if it is proven that the employer failed to verify the employee's job qualifications.[165] In order to avoid hiring individuals without first having a thorough knowledge of their character, managers are urged to go beyond listed references when doing background checks for pre-employment screening. Personnel departments often feel obliged to contact anyone who might be familiar with the person, including former employees, neighbors, or anyone else who has had an established relationship with the individual.[166] Increasingly, companies are also checking the personal credit reports of job seekers in an attempt to gauge the integrity of prospective employees.[167]

In practice, information flows freely among employers, personnel managers having their own rather close-knit fraternity. In addition, it is not uncommon for some supervisors to bypass the personnel department altogether in checking on an applicant by directly contacting the candidate's former supervisor. The employee has no way of knowing this is going on. One technique which gives rise to abuse is the use of the pretext interview. In such interviews, investigative firms making employee background checks encourage agents to misrepresent themselves and the reason for the interview in order to elicit candid information.[168] When private agencies are used to check the histories of employees or job applicants, investigators talk with neighbors, business colleagues, associates, former employers, and former teachers, then submit their reports which, unverified, tend to be only as reliable as the informant or the individual making the check.[169]

In some cases, individuals are victimized by unreasonable decisions triggered by computer-stored information.[170] In one case, a

---

164. English, *supra* note 140.

165. Manley, *The Employer's Burden*, INC., Sept. 1989, at 125. *See generally* Linowes, *Employee Rights to Privacy and Access to Personnel Records: A New Look*, 4 EMPLOYEE REL L.J. 34 (1978) (findings and recommendations of the Privacy Protection Commission regarding employee privacy).

166. Manley, *supra* note 165.

167. Fuchsberg, *More Employers Check Credit Histories of Job Seekers to Judge Their Character*, Wall St. J., May 30, 1990, at B1, col. 3.

168. PRIVACY PROTECTION STUDY, *supra* note 113, at 240.

169. *Id.* at 332.

170. PRIVACY IN AMERICA, *supra* note 22, at 25.

seventeen year old girl was denied a job as a clerk in a large department store because a computer revealed that she had been caught shoplifting when she was twelve years old.[171] Even though she had not been arrested or convicted, and there had been some doubt concerning the identity of the shoplifter, the fact that the incident was part of the record labeled her a security risk.[172]

M. Medical Records

An employee using the medical services offered by an employer does so at some risk to the traditional confidential relationship between physician and patient, unless precautions are taken to protect the confidentiality of that relationship from the usual work-related responsibilities of the medical department.[173]

Corporate physicians are sincerely concerned about possible misuses of the employee medical records they maintain.[174] But no matter how hard they strive to be independent, their allegiance is ultimately to the employer.[175] Some large employers have procedures that guarantee the confidentiality of medical record information in all but the most extreme circumstances; and many corporate medical departments only make recommendations for work restrictions, releasing diagnosis or treatment details in only the most urgent cases.[176] Nevertheless, it is the corporate doctor's duty to inform the employer of an individual's condition when the interests of the employer or other employees could be adversely effected.[177]

The problem of medical treatment confidentiality has been exacerbated in recent years due to an increasing number of small and medium-sized businesses processing insurance claims in-house.[178] The advent of computers has also made it easier for employers to keep tabs on employees' utilization of insurance benefits.

One way to correct this problem is to bypass the employer's personnel office by sending insurance claims directly to the carrier where personnel are not co-workers of the patient and are more likely to be trained to maintain confidentiality. The International Business Machines Corporation, for example, has successfully implemented privacy protection by this means.[179] The only data the em-

---

171. *Id.*
172. *Id.*
173. PRIVACY PROTECTION STUDY, *supra* note 113, at 266-67.
174. *Id.*
175. *Id.*
176. *Id.*
177. *Id.*
178. Linowes, *supra* note 165, at 36-67.
179. Arnst, *Users Say Privacy Measures Make Good Business Sense*, COMPUTERWORLD, Oct. 31, 1977, at 4, col. 2. *See also Employment & Personnel Record-*

ployer receives are periodic statistical analyses without any individuals identified.

N. Security Records

Security records differ from the usual personnel records in that they are often created without the employee's knowledge.[180] Sometimes the information in them is inconclusive, or the problem that precipitated the record is not quickly resolved.[181] Nonetheless, an employer may have to maintain security records to safeguard the workplace or corporate assets.[182] Security departments traditionally cooperate with personnel departments in investigating incidents involving employees.[183] Where the security and personnel functions are separate, however, security records are often filed by incident and not by individual.[184] Since these records have little, if any, impact on personnel decisions about an employee, giving supervisors or employees free access to them might be difficult to justify.[185] However, where security records are used for discipline, termination, promotion, or evaluation, fairness dictates that the employee be made cognizant of the file and given the opportunity to challenge, correct, and add comments to it.[186]

IV. The Corporation in Society

A. Social Responsibility

In all of this, who should society look to for privacy protection—the immediate supervisor, top executive, or the corporation itself? The answer could significantly change how privacy rights are perceived and enforced in the workplace.

Although it is common to view a corporation solely as a collection of material things, the true substance of the corporation is as a collective effort of individuals. It is essentially a human or social organization. It is the natural person component, more so than the material component, that is the key to a corporation's existence.[187]

The corporation as a collective enterprise is entitled to all the

---

keeping Practices: Hearings Before the Privacy Protection Study Commisssion, 282-328 (1976) (testimony of Walter E. Burdick, Vice President, International Business Machines Corp.).

180. Privacy Protection Study, *supra* note 113, at 265-66.
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.* As a rule, these records are not available to management. *Id.*
185. *Id.*
186. *Id.*
187. R. Hessen, In Defense of the Corporation 40-41 (1979).

legal privileges and obligations attributed to natural persons, including a right to privacy.[188] "Concepts and functions normally attributed to persons can also be attributed to organizations made up of persons," argue Kenneth E. Goodpaster and John B. Matthews, Jr., of Harvard University.[189] Therefore, we should require these organizations to have the same moral attributes we require of ourselves. The Supreme Court in *Hale v. Henkel*[190] held that corporations are protected by the same constitutional safeguards as individuals. Corporate entities have interests identical to those of other members of society, and like natural persons, can be adversely affected by a loss of personal privacy.[191] Therefore, if corporations enjoy privacy safeguards as citizens, they can logically be expected to respect the privacy of others.[192]

Business decisions have social consequences and cannot be solely economic acts, writes Professor Keith Davis of Arizona State University.[193] Business is obliged to act in ways which will protect the interests of society. Corporations that ignore the responsibility of their social power run the risk of losing any power they have. According to Davis, "business institutions as citizens have responsibilities for social involvement in areas . . . where major social needs exist."[194] Thus, business must bear its share of the costs of citizenship and benefits from the better society that results.[195] Society has entrusted many of its resources to business and expects proper trusteeship in return.[196] Similarly, social responsibility applies to all people regardless of their life roles.[197]

To a large extent, driving the mandate for re-balancing the relationships between corporations and society are pressures by labor unions, consumer groups, and government regulatory bodies.[198] Not to be overlooked is the enlightened self-interest of policy-making executives who are integral parts of the corporate structure.[199] They

---

188. *Id.* at 83-85.

189. Goodpaster & Matthews, *Can a Corporation Have a Conscience?* in BUSINESS ETHICS, 157 (W. Hoffman & J. Moore, eds. 1984).

190. 201 U.S. 43 (1906).

191. R. HESSEN, *supra* note 187, at 84-85.

192. *Id.*

193. The following material on the corporation's role in society was included appeared in an address entitled *Corporation as Citizen* delivered to the ninth international symposium on Consitutional Roots, Rights and Responsibilities at the Smithsonian Institution in Washington, D.C. May 22, 1987. *See* Linowes, Corporation as Citizen, Corporate Board, May/June 1988, at 7.

194. Davis, *An Expanded View of the Social Responsibility of Business*, in ETHICAL THEORY AND BUSINESS 95 (T. Beauchamp & N. Bowie, eds. 1983).

195. Linowes, *supra* note 193.

196. *Id.*

197. *Id.*

198. *Id.*

199. *Id.*

are well-educated, loyal American citizens who are concerned about the welfare of our nation and its future, and they imbue their corporate entities with the same sensibilities.[200]

Corporations benefit from numerous opportunities in this country because they function in an open and free society with only limited regulation. Some argue these opportunities permit the remarkable successes American corporations have achieved.[201] We are justified, therefore, in expecting to receive in exchange a recognition by corporations of a duty to act for the common good. Corporations are asked to give back to society—over and above their industrial productivity—a fair share for what they receive. A full set of reciprocals is being called for in a new articulation of the corporate social contract.[202]

B. Fair Information Practices

Three main public policy objectives in relations between individuals and the organizations with which they deal are to minimize intrusiveness, to maximize fairness, and to create a legitimate and enforceable expectation of confidentiality when this expectation is warranted.[203] These policies clearly pertain to the employment relationship. Too many leading corporate institutions are not practicing fair information policies toward their own personnel. Many of them do not even conduct periodic evaluations of their personnel record keeping systems.

An employer should periodically and systematically examine its employment and personnel record-keeping practices, including a review of:

(1) the number and types of records it maintains on individual employees, former employees, and applicants;

(2) the items of information contained in each type of employment record it maintains;

(3) the uses made of the items of information in each type of record;

(4) the uses made of such records within the employing organization;

(5) the disclosures made of such records to parties outside the employing organization;

(6) the extent to which individual employees, former employ-

200. *Id.*
201. *Id.*
202. *Id.*
203. The recommendations regarding fair information practices originally appeared in PRIVACY IN AMERICA, *supra* note 22.

ees, and applicants are both aware and systematically informed of the uses and disclosures that are made of information in the records kept about them.

1. Disclosures of Personal Employment Data

Although a right of privacy concerning records held by third parties has not been broadly recognized by the courts,[204] an employer should limit external disclosures of information in records kept on individual employees, former employees, and applicants. It should also limit the internal use of such records.

2. Individual Access

An employer should permit individual employees, former employees, and applicants to see, copy, correct, or amend the records maintained about them, except for highly restricted security records, where necessary. An employer should assure that the personnel and payroll records it maintains are available internally only to authorized users on a need-to-know basis.

3. Informing the Individual

An employer, prior to collecting the type of information generally collected about an applicant, employee, or other individual in connection with an employment decision, should notify the individual as to:

(1) the types of information expected to be collected;

(2) the techniques that may be used to collect such information;

(3) the types of sources that are expected to be used;

(4) the types of parties to whom and circumstances under which information about the individual may be disclosed without authorization, and the types of information that may be disclosed;

(5) the procedures established by statute by which the individual may gain access to any resulting record;

(6) the procedures whereby the individual may correct, amend, or dispute any resulting record.

An employer should clearly inform all its applicants upon request,

---

204. The Supreme Court, for example, held in U.S. v. Miller, 425 U.S. 435 (1976), that an individual's fourth and fifth amendment protections do not extend to government requests for financial records maintained by organizations. *See* Linowes & Bennett, *Privacy: Its Role in Federal Government Information Policy*, LIBRARY TRENDS, Summer 1986, at 30 (court enforcement of the Privacy Act).

and all employees automatically, of the types of disclosures it may make of information in the records it maintains on them, including disclosures of directory information, and of its procedures for involving the individual in particular disclosures.

4. Authorizing Personal Data Disclosure

No employer should ask, require, or otherwise induce an applicant or employee to sign any statement authorizing any individual or institution to disclose information about the individual, unless the statement is:

(1) in plain language;

(2) dated;

(3) specific as to the individuals and institutions authorized to disclose information;

(4) specific as to the nature of the information authorized to be disclosed;

(5) specific as to the individuals or institutions to whom information is authorized to be disclosed;

(6) specific as to the purpose(s) for which the information may be used;

(7) specific as to its expiration date, which should be for a reasonable period of time not to exceed one year.

5. Medical Records

An employer that maintains an employment-related medical record about an individual should assure that no diagnostic or treatment information in any such record is made available for use in any employment decision. However, in certain limited circumstances, special medical information might be so used after informing the employee. Upon request, an individual who is the subject of a medical record maintained by an employer, or another responsible person designated by the individual, should be allowed to have access to that medical record, including an opportunity to see and copy it. The employer may charge a reasonable fee for preparing and copying the record. An employer should establish a procedure whereby an individual who is the subject of a medical record maintained by the employer can request correction or amendment of the record.

6. Polygraph Use

Employers should not use a polygraph or other truth-verification equipment to gather information from an applicant or em-

ployee. As observed earlier, the Employee Polygraph Protection Act of 1988 prohibits the use of lie detectors in pre-employment screening and for random testing of employees in the private sector.[205] Only pharmaceutical companies and firms employing security guards in areas related to "health or safety" are exempt from the ban.[206] The federal law also establishes guidelines for the administration of lie detector tests which stipulate that each test be at least an hour and a half long and that examiners administer no more than five tests in one day.[207] All test questions must be discussed with the subject in advance. Questions may not be altered during the exam, and inquiries about religious, political, or union affiliation are not allowed.[208]

7. Use of Investigative Firms

Each employer and agent of an employer should exercise reasonable care in the selection and use of investigative organizations, so as to assure that the collection, maintenance, use, and disclosure practices of such organizations fully protect the rights of the subject being investigated.

8. Arrest, Conviction, and Security Records

When an arrest record is lawfully sought or used by an employer to make a specific decision about an applicant or employee, the employer should not maintain the record for a period longer than specifically required by law, if any, or unless there is an outstanding indictment. Unless otherwise required by law, an employer should seek or use a conviction record pertaining to an individual applicant or employee only when the record is directly relevant to a specific employment decision affecting the individual. Except as specifically required by federal or state statute or regulation, or by municipal ordinance or regulation, an employer should not seek or use a record of arrest pertaining to an individual applicant or employee. Where conviction information is collected, it should remain separate from other individually identifiable employment records so that it will not be available to persons who have no need of it. An employer should maintain security records apart from other records.

---

205. 29 U.S.C. §§ 2001-2009 (1988).
206. *Id.*
207. *Id.*
208. *Id.*

CONCLUSION

Some people may argue that the burden of implementing privacy safeguards would be yet another unnecessary drag on the operations of business—that the forces of efficient management run counter to the forces of human privacy protection. Nothing can be considered right from the standpoint of efficiency if it is wrong morally. Those who think there is a basic conflict between long-term management effectiveness and safeguarding personal privacy rights must either be inexperienced in the art and science of management or ignorant of the consequences of personal privacy abuses. Full freedom is as necessary to the health and vigor of business as it is to the health and vigor of citizenship.

On several fronts, steps are being taken to protect employee privacy. The city of San Francisco, for example, enacted an ordinance in 1986 which protects workers in the private sector from indiscriminate drug testing.[209] Under the San Francisco law, no employer can require employees to submit to any blood, urine, or encephalographic test for drug use unless there is evidence that the employee's faculties are impaired and workplace safety is jeopardized.[210] If a drug test is deemed necessary, the employee may request testing by an independent laboratory and is given an opportunity to rebut the results.[211]

Many of the nation's largest and most progressive corporations now have voluntarily initiated information policies designed to ensure the privacy and confidentiality of employee records to the maximum degree possible.[212] The International Business Machines Corporation ("IBM"), for instance, believes its concerns about privacy make good business sense because initiatives in this area have improved employee relations. The quantity of data in the company's personnel files has been pared to a minimum. Such personal data as payroll deductions, life insurance, home ownership, mortgages, and wage garnishments are classified as "non-worker-related" and are not available, even to supervisory people. Information dealing with arrest and convictions is used for security purposes only.

IBM keeps its files as current as possible. Data concerning training grades and conviction records are destroyed after three years. Employees are provided on request with a computer printout

209. *Drug Testing in the Workplace*, Civ. Liberties, Spring 1986, at 5, col.1.
210. *Id.*
211. *Id.*
212. The following information on practices observed by IBM, Equitable Life Assurance, Bank of America, and Citibank appeared in PRIVACY IN AMERICA, *supra* note 22, at 30.

of their personal file. With regard to medical records, employees have full access to information kept for government requirements or concerning voluntarily requested examinations. Doctors' notes, however, are only reviewed with the employee by the doctor. Where outside inquiries are made, IBM will only verify employment and will not release salary or performance data without the employee's written consent. If personal information is requested by a law enforcement agency, an individual determination on compliance is made in each case.

At the Equitable Life Assurance Society, where a major restructuring of personnel policies took place, only nine items are included in the personnel files. These include only job-related material, such as employment applications, leave of absence requests, and salary actions. Ford Motor Company personnel are invited to help keep data in their employment files current by advising the company of educational progress and other achievements which could affect their potential for future promotions. In addition, salaried employees can put statements in their personnel files expressing interest in specific positions or developmental opportunities.

Giving employees access rights to their personnel files is a part of Bank of America's stated employee relations policy. The company is convinced that openness is the best way to instill employee confidence. Similarly, Citibank voluntarily adopted fair information practices for all its personnel records. As a result, the efficiency of the operations of the personnel department was improved, and the costs reduced. All extraneous data previously accumulated in individual personnel files were removed and irrelevant information is no longer being collected.

Companies can avoid costly litigation as well as reap considerable goodwill and operational benefits by adopting fair information practices. These practices can help protect the privacy rights of all individuals with whom the corporation comes in contact. Every effort should be made to safeguard personal privacy while meeting legitimate business needs. Unfortunately, firms with such wholesome guidelines represent a limited number of the total work force in America. Thousands of other large, medium and small organizations employing many millions of people have not yet responded. Employers should not await a government mandate. Immediate action should be taken to address workplace privacy concerns.