

GEORGETOWN UNIVERSITY
SCHOOL OF CONTINUING STUDIES
BACHELOR OF ARTS IN LIBERAL STUDIES PROGRAM

ELECTRONIC THESIS RELEASE FORM

Student name: PAUL E. HARRISON
Thesis title: PRIVACY IN THE WORKPLACE - THE EMPLOYEE-EMPLOYER RELATIONSHIP

I hereby grant to Georgetown University and its agents the non-exclusive license to archive and make accessible my thesis in whole or in part in all forms of media, now or hereafter known. I retain all ownership rights to the copyright of the thesis, including the right to use it in whole or in part in future works. I authorize Georgetown University to archive my electronic thesis and to release the entire work immediately for access worldwide.

Author signature: _____

Date: 10/10/08

FAY
MR. HANNA
202-687-8954

GEORGETOWN UNIVERSITY
SCHOOL FOR SUMMER AND CONTINUING EDUCATION
UNDERGRADUATE LIBERAL STUDIES PROGRAM

The thesis of Paul E. Harrison entitled
The Right to Privacy: A Strategic Ethical
Issue in Employee-Employer Relations

submitted in partial fulfillment of the requirements for the
degree of Bachelor of Arts in Liberal Studies in the School
for Summer and Continuing Education of Georgetown University
has been read and approved.

Douglas M. McCabe
Mentor(s)

Dr. Kayla Callahan
Director, Liberal Studies Program

April 28, 1995
Date

The Right to Privacy: A Strategic Ethical Issue in
Employee-Employer Relations

A Thesis
submitted in partial fulfillment of the requirements for
the degree of
Bachelor of Arts in Liberal Studies

By

Paul E. Harrison

School for Summer and Continuing Education
Georgetown University
Washington, DC
May 1, 1995

ABSTRACT

Privacy is thought to be one of the most fundamental American rights as guaranteed by the U.S. Constitution. However, the Fourth Amendment's scope is limited to protection from the government and does not address the citizen-to-citizen privacy relationship as it exists in the private sector workplace. Consequently, vastly different conclusions are reached by both employees and employers over the "right" to and degree of privacy that should exist in the workplace.

In the absence of a clear and universal legal definition of privacy or the conditions under which privacy ought to exist, the debate over privacy is fraught with values judgments and as such, becomes an ethical issue. For purposes of discussion, privacy is defined as the freedom from the unknown or unauthorized intrusions of others into one's affairs.

Technological developments provide tools for employers to use in the collection and use of employee information,

drug and honesty testing, and employees surveillance. At issue in this debate for the employer is the protection of her interests and assets, and maintenance of a high degree of autonomy in business decisions. For the employee, great concern exists over the intrusive nature of the employers' methods of policing activities both on the job and off, and the desire to maintain a degree of personal privacy and individual autonomy.

After examining the employers' and employees' positions together, a balance was found to be possible that considers the needs of the employer, the rights of the individual, and the greater good of society. Guidelines such as full disclosure of privacy policy at the pre-employment stage and thorough communication of privacy policy to existing employees help achieve this balance. These types of proactive policy decisions minimize economic loss to employers thus promoting the greater good of society while still allowing employees to make conscious and voluntary employment decisions if an employer's privacy policy is not satisfactory.

ACKNOWLEDGMENTS

The completion of this thesis marks a special point in my life. A point that provides an opportunity to tell my mother how much I appreciate her love and sacrifice over the past twenty-eight years. I thought this day would never arrive. I love you, Mama.

TABLE OF CONTENTS

ABSTRACT	ii
ACKNOWLEDGMENTS	iv
Chapter	
1. THE PROBLEM	1
2. DEFINITION	8
3. AVENUES OF INVASION OR TOOLS OF EFFICIENCY?	10
Collection and Use of Employee Information	
Drug and Honesty Testing	
Employee Surveillance	
4. CONCLUSION AND FRAMEWORK	23
Privacy Policy Guidelines	
SELECTED BIBLIOGRAPHY	29

Chapter 1

THE PROBLEM

"There is no general federal or state law creating or protecting a 'zone of privacy' in the workplace. The U.S. Constitution's First Amendment free-speech clause and the Fourth Amendment protection against 'unreasonable searches and seizures' apply only to actions by the government, not to private sector employers...[private sector] employees leave their constitutional rights at the workplace door."¹

Privacy is thought to be one of the most fundamental American rights. Many believe that privacy, or "the individual's right to be let alone,"² is guaranteed by the Constitution. However, the Constitution does not address the issue of individual privacy as a specific right, nor is there any mention of what criteria constitute workplace privacy.

¹Webster, George D., "Respecting Employee Privacy," Association Management 46, (January 1994): 142.

²Linowes, David F., Privacy in America: Is Your Private Life in the Public Eye?, (Chicago: University of Illinois Press, 1989), 13.

The Fourth Amendment provides for "the right of the people to be secure in their persons, houses, papers, and effects, [and protection from the Government] against unreasonable searches and seizures." Hence, the Fourth Amendment serves to restrict governmental intrusion but does not address private sector, or citizen-to-citizen, privacy.

The vastly different conclusions reached by employers regarding employees' "right" to privacy have propagated intense debate in recent years as a result of Western society's entrance into the Information Age. Technological advances have given government and private employers alike new and easier opportunities to collect, compile, retrieve and store enormous amounts of diverse information. Data are collected about potential and current employees' criminal activity, credit and medical histories, marital status, drug use and many other areas.

This same technology affords employers relatively inexpensive methods with which to track an employee's activities while at work and even at home. Employee

monitoring has become commonplace with the use of video cameras, security codes, and electronic eavesdropping on phone conversations and electronic mail (e-mail).

Drug testing has raised concerns of employers policing the off-hours behavior of employees. Yet while employees are concerned for their privacy, employers find themselves held increasingly accountable for the behavior of their employees. Justification for employers' use of background investigations and employee monitoring comes from the possibility of civil liability cases targeting negligent hiring and management practices.

During work hours, and in some cases during off hours, an employee who has an accident while under the influence of drugs or alcohol or who erupts in a fit of violence with an automatic rifle precipitates scrutiny of the employer's hiring practices and claims of negligence against the employer on the part of the victim or the victim's family. Corporate resources are easy targets for these lawsuits.

Further justification for employers' use of these new technologies comes from lost revenues in the form of theft,

vandalism and loss of trade secrets and other proprietary data. The U.S. Chamber of Commerce estimates that the annual loss to employers is in the neighborhood of \$40 billion for employee theft alone.³ Consumers ultimately pay higher prices for goods and services to offset these losses making employee theft an area of concern for all consumers. This figure does not consider losses due to shoplifting, employee sabotage or poor performance. Estimates for these types of losses alone may easily exceed the \$40 billion figure.

Minimization of losses due to poor performance and sabotage can be achieved by management's continual observation of an employee's routine through which inefficient activities can be curtailed. Employees who sleep on the job and further take advantage of employers can be disciplined or otherwise eliminated through the use of surveillance.

³Warner, David, "The Move to Curb Worker Monitoring," Nation's Business 81, (December 1993): 38.

Electronic surveillance has provided a vehicle for management to be much more efficient. One manager is now able to observe many more employees than if she had to personally visit and observe each one. Also, employees can work normally without the presence of a supervisor standing over their shoulders. For employees who work as they are expected, there may be little need for concern.

Working for a manager behind a desk or behind a camera lens simply represents a changing paradigm. The adversarial relationship that exists between workers and management creates a tense, even paranoiac, atmosphere with regard to privacy. Tension aside, even the happiest and most "empowered" employees can feel that an employer is too intrusive upon their work activities.

Privacy invasion, then, becomes a question of individual acceptability and as such is "fraught with judgment calls about our own privacy rights versus other people's rights."⁴ Consistent with the subjectivity of

⁴Carroll, Archie B., Business & Society: Ethics and Stakeholder Management, (Cincinnati, Ohio: South-Western Publishing, 1993), 441.

privacy invasion, any definition of privacy involves a subjective ideal which may be difficult, if not impossible, to achieve. Indicative of this difficulty is the fact that "there are no clear legal definitions of what constitutes privacy or privacy invasion."⁵

In the absence of a clear and universal legal definition, privacy becomes a values judgment, an ethical issue. Nowhere is this ethical issue more apparent than in the non-union, private sector workplace.

It will be important to first establish a definition of privacy, an ideal, and examine how that definition applies to the non-union, private sector workplace. It will also be important to determine if the right to privacy ought to apply in this relatively Constitutionally-unprotected realm. Equal consideration must be given to both sides of the issue - employer and employee - and must result in a position that serves the greater good of society.

⁵Ibid., 440.

Any discourse that seeks to explore privacy is obligated to provide a working definition, for without one there is no point of reference for the reader. Many current articles discussing privacy invasion or the right to privacy fail to explain what is meant by privacy and thus result in ambiguous conclusions. This definition is provided in the next chapter.

By no means will this limited undertaking seek to debate the overall need for privacy and personal space, nor will the discussion exhaustively retrace the historical precedence in developing privacy legislation. Simply stated, this treatise will examine the ethical implications of the methods employers currently use to monitor employees' activities both on and off the job and conclude with a position on the degree of privacy required in the workplace and the framework within which this degree of privacy can be obtained and maintained.

Chapter 2

DEFINITION

It is easy to understand that the presence or exercise of "privacy," in a sense, "limits the control of others over our lives."⁶ In this way, an individual's autonomy is maintained. Yet in society, there must be limits to individual freedom to the extent that others' rights are not compromised; a completely free society would result in chaos.

From this standpoint then, it is important to recognize that there must be a balance between the good of society and the rights of the individual. Legislation seeks to maintain this balance in the greater realm of society and more recently, in the workplace. The question though, is whether privacy is a feasible consideration in the private sector workplace.

⁶Schoeman, Ferdinand, D., Privacy and Social Freedom, (New York: Cambridge University Press, 1992), 1.

Developing laws that represent a compromise between employer duty and employee rights is difficult at the very least. Of paramount importance to the employer is liability for their employees' actions and responsibility to corporate shareholders. The employee would like to think that his private life is just that, private. But that still leaves the question as to the definition of privacy.

As derived from its Constitutional roots and its resulting condition, privacy, in its ideal form, is defined as the absence of others' control or intrusion in one's life. There are instances where there needs to be others' control in one's life, such as in society and in the workplace. With pragmatic consideration, the workable definition of privacy is to be free from the unknown or unauthorized intrusions of others into one's affairs.

Chapter 3

AVENUES OF INVASION OR TOOLS OF EFFICIENCY?

This section of the discussion will examine three tools that employers use in attempts to reduce potential liability and losses of revenue due to theft and other factors. These tools are: collection and use of employee information; drug and honesty testing; and electronic surveillance.

Collection and Use of Employee Information

Businesses tend to be very "nosy" when it comes to the collection of employee information, especially in employee background investigations. "Some employers are delving further into employees' personal lives, and employees are fighting harder for the right to be let alone."⁷ To complicate matters, "few clear guidelines exist for

⁷Lissy, William E., "Workplace Privacy," Labor Law for Supervisors 54, (October 1993): 20.

determining what constitutes a violation of privacy in the workplace."⁸

Because of potential liability issues, "firms point to the increasing reluctance of the former employers of job applicants to provide reliable references."⁹ Companies are forced to protect their interests by trying to uncover larcenous tendencies, an unpredictable temper, and even asocial behavior. Former employers do not want to risk a defamation of character lawsuit by revealing information other than dates of employment. Employers' resources make attractive targets for liability suits necessitating proactive, pre-employment background investigations.

The right to privacy, defined as the right to be free from unauthorized or unknown intrusion into one's affairs, can be maintained in the case of the collection and use of employee information if the employer fully discloses to the employee what information will be collected and the purpose for which it will be used. The prospective employee will

⁸Ibid.

⁹"Don't Pry," The Economist 317, (October 6, 1990): 18.

have the choice to reconsider her option of pursuing the job before allowing the employer to proceed with any investigation.

However, a violation of privacy may still occur when an employer's intrusion into the private affairs of an employee, disclosed or otherwise, could be considered highly offensive to a reasonable person.¹⁰ The ambiguity of the term "reasonable" provides room for interpretation and uncertainty.

Liability issues regarding the confidentiality of employee information extend beyond the simple collection and storage of information. A great deal of concern exists with the assimilation of that data for purposes other than intended. Compiled information can reveal considerably more about an employee than the components alone. In this respect, privacy implications extend far beyond the workplace and attest to the need for a balance between the employers' need for information and individuals' right to privacy.

¹⁰Lissy, "Workplace Privacy," 20.

"Courts expect employers to balance the employee's right of privacy with their own need for job-related information."¹¹ Employer-operated employee assistance programs pose potential diversions from the courts' expectations. Over eighty percent of Fortune 500 companies have employee assistance programs in place, creating a great deal of potential for breach of privacy.¹² Confidentially disclosed information regarding drug abuse, psychological instability or homosexual tendencies, in many cases, is kept in the same types of accessible data banks as other employee information. The interconnectivity of computer networks allows for unauthorized access not only from within the organization but also by outsiders. Unauthorized users of this information present very real privacy infringement issues for both the employee and the employer.

¹¹Bahls, Jane E., "Checking Up on Workers," Nation's Business 78, (December 1990): 30.

¹²Gregory C. Parlman and Erica L. Edwards, "Employee Assistance Programs: An Employer's Guide to Emerging Liability Issues," Employee Relations Labor Law Journal 17, (Spring 1992): 594.

Work decisions, such as consideration for promotion, could be unfairly influenced by the discovery of a drug problem. Such a scenario provides an example of the potential to use information for purposes other than those for which it was intended. This misuse of information raises important ethical issues.

For the employer, a drug-addicted employee may become a significant liability in a supervisory capacity or any other position. The paternalistic nature that most companies assume encourages employees to seek assistance to eliminate their problem while still working. Employees with drug addictions and other severe psychological problems become significant liabilities to the employers. Employers must invest considerable faith and resources in the success of employee assistance programs. In the case that these programs are not successful an employee's actions may put the employer at higher risk for liability lawsuits.

Compounding the issue is the collection and use of employee information sanctioned by federal and state

governments. Private sector employers are charged with the task of collecting information and, in some cases, alimony and child support payments on behalf of government agencies. The Internal Revenue Service, Social Security Administration, and state unemployment offices are just a few of the agencies that mandate employer-collected information.

Requirements placed upon employers by federal, state and local governments to collect information about employees are constantly changing and expanding. Through private employers, the government is finding new opportunities to delve into citizens' private lives. These actions completely skirt the protection of the Fourth Amendment, but that is another issue.

Drug and Honesty Testing

Drug and honesty testing are considered the most invasive of the privacy issues and as such have been more adequately addressed by law. In response to employees' concerns over the invasive nature and accuracy of the

polygraph, Congress enacted the Employee Polygraph Act of 1988 that served to ban nearly all private sector uses of lie detectors. The only exceptions are as follows:

"A test may be administered to existing employees in the course of an employer's ongoing investigation of economic loss, and under certain circumstances...private security and drug manufacturing industries may conduct pre-employment polygraph examinations."¹³

Employers, however, concerned for economic loss due to dishonesty, found a new honesty tool, the written integrity test.

Related to the polygraph, written honesty or integrity tests are supposed to achieve the same results as the polygraph. Such tests "typically pose eighty or ninety statements [to] which the employee or applicant is asked to agree or disagree."¹⁴ The answers to these questions, many of which are the same question but simply rephrased, are used to determine an examinee's level of honesty.

Employees have begun to question the invasiveness and validity of written tests. It may just be a matter of

¹³Carroll, Business & Society, 444.

¹⁴Ibid.

years before Congress amends the Polygraph Act to include written tests. The push to outlaw written exams has been slow, probably because of the non-intimidating nature of the written test. Employees may even feel that the written test makes it easier to conceal information. This matter is still open for debate. The legitimacy of drug testing remains open for debate as well.

Drug testing, usually through urinalysis, has been contested by employees for many years. Drug testing is considered to be the most invasive of employers' methods for policing behavior. This feeling of invasiveness surrounds the extraction of bodily fluid for analysis. This aspect stirs strong feelings of privacy invasion. Many companies restrict testing to prospective employees by consent only. Of course, failure to consent disqualifies one from possible employment.

At issue for the employers is the loss of lives and money that drug use and abuse is proven to cause. Weak Federal support for drug testing comes in the form of the Drug-Free Workplace Act of 1988. This legislation

mandates no action and simply asks employers to provide a good-faith effort to maintain a drug-free workplace.¹⁵

Estimated employer losses due to alcohol and other drugs are \$100 billion a year.¹⁶ Public safety areas such as the transportation industry are particularly concerned about safety because lives are at stake.

The impetus for legislation to regulate drug testing is coming from the state and local levels of government. The trend is to "restrict or prohibit random testing of current employees, except when safety is the issue."¹⁷ This policy is entirely consistent with concern for the greater good of society over the individual. The right to privacy is still intact with regard to drug testing, as prospective employees are free to occupy jobs that do not entail drug testing or the public's safety. If current employees are exempt from testing, those same employees

¹⁵Ibid., 448.

¹⁶Parliman, "Employee Assistance Programs," 593.

¹⁷George R. Gray and Darrel R. Brown, "Issues in Drug Testing for the Private Sector," HR Focus 69, (November 1992): 15.

would have the option of staying in that job so as to be free from an employer's intrusion upon their affairs.

Employee Surveillance

Phone monitoring is perhaps the most common form of employee surveillance. The Federal Wiretap Law "permits employers to listen to calls 'in the ordinary course of business.'"¹⁸ However, employers are not permitted to listen once a call is determined to be personal in nature.

"More than one company in five eavesdrops electronically on its employees."¹⁹ Whether for purposes of customer service or to ensure that company phones are not being used for private conversations, there can arguably be a valid "need" for employers to monitor employees' conversations. The problem that exists today is that there is no clear line between "permissible monitoring and illegal snooping."²⁰ Congressional legislation in the form of S. 984 and H.R. 1900 is attempting to deal with

¹⁸Jacobs, Deborah L., "The Perils of Policing Employees," Small Business Reports 19, (February 1994): 26.

¹⁹Ibid., 23.

²⁰Ibid., 24.

this area. However, the effort has failed over the past few years and there is no reason to expect this archaic and arbitrary legislation to become law anytime soon.

Other forms of surveillance include miniature microphones and cameras that are readily available for use by employers. Cameras are now so small that they can easily be hidden in an office fire sprinkler head or a bathroom soap dispenser. These types of technological advances are occurring at a rate that far exceeds the creation of legislation to address them. These devices allow for easy and cost effective observation of employees' activities while on the job.

The area of employee surveillance favors the employer. The property and equipment used during the course of business, in most cases, belongs to the employer. It is difficult for employees to argue they should have free use of and reign over an employer's property.

Supporting the employers' position is the point that employees, considered "wage slaves" by Karl Marx, are paid

by the employer according to some value placed upon the worth of their function to an organization. In some settings, workers require much more latitude with regard to free thought in order to perform their jobs, but this is entirely at the discretion of the employer.

If an employee conducts personal business during those hours in which she is being paid by the employer for her time, there is legitimate reason to label this lost time as theft. Although, a one minute conversation with the school nurse explaining to a parent that her child is ill seems minor compared to hours spent operating a personal enterprise at the employer's expense, but both are theft nonetheless.

Many employers make allowances for personal business whether that means granting personal leave to resolve personal problems or providing a pay phone outside of the office area where employees are free to place calls and conduct personal business during non-work hours. While the employee has a right to privacy, the employer also has a right to protect her interests.

The right to privacy implies the right to be free from the unknown or unauthorized intrusion of others into one's affairs. In this sense, the employer must simply inform the employee that certain types of monitoring will take place. An employee who does not agree can take his skill to another employer who does not use surveillance. Granted, the job may not be of equal pay or in the same profession, but the point is that all non-union, private sector employees are free to seek other employment if a privacy policy is not satisfactory.

Chapter 4

Conclusion and Framework

Employers are obligated by corporate responsibility and driven by profit to take action to curtail immense, and in most cases immeasurable, losses due to theft, liability, drug abuse and inefficiency. These actions - collection of employee data, drug and honesty testing, and employee surveillance - can lead to feelings of privacy invasion on the part of employees. The idea that an individual has a right to privacy in the workplace has proven to be entirely possible.

Employees are paid to perform a function important to the employer. It is imperative to consider that employees are making a conscious decision to "sell" their time to the employer and the employer "owns" and has responsibility for employees during these paid hours.

The situations in which employers most often find

themselves facing legal battles occur when employees are given or developed a sense that there was a "reasonable expectation" of privacy that was suddenly changed without notice. Since the definition of privacy is not clear outside of this paper, employers can often be found by the courts to be at fault for privacy invasion and open for civil settlements. It is in the best interest of employers to avoid lawsuits, as even the winners must pay legal costs totaling hundreds of thousands of dollars.

An employee's best interests are served by knowing what to expect of his employer. Employees have a vested interest in their employer's continued operation, which can be maintained only as long as the operation remains profitable. It is important for the employer to inform employees of what is expected from them. Animosity and confusion do not serve the bigger interests of the organization or the employee. In order to eliminate this anxiety and reduce the possibility of privacy invasion lawsuits, a privacy framework is detailed below that first

defines privacy and then sets guidelines for the creation of policy for protecting employee privacy. If employees know the level of privacy granted by the employer prior to accepting employment, they could make a conscious choice prior to accepting employment as to whether that level of privacy is acceptable.

Legislation will not solve the workplace privacy issue. Assigning arbitrary limits and stipulations to work routines cannot possibly account for every job situation or market dynamic available. The labor market is free to shift to those companies with less restrictive or no privacy policies. For those people who are not satisfied with an employer's privacy policy there are options such as a job change, the prospect of self-employment, or remaining with the firm and working to change the unacceptable aspects of the policy.

Extensive surveillance is bound to be made available by new technologies, the likes of which we cannot imagine today. The current rift between employers and employees simply represents a changing paradigm. The transitions can

be smoothed simply by informing employees, in the pre-employment stages, of the company policies and practices and elaborate on the expectations of employment and the consequences of failing to meet those expectations.

"Employment-at-will" employees are free to seek other employment as seen fit.

Privacy Policy Guidelines

Privacy - To be free from the unknown or unauthorized intrusion of others into one's affairs.

In general:

1. Development of a comprehensive privacy policy.
2. Effective communication of privacy policy to all applicants and employees.
3. Fair notice must be given to all employees prior to the installation of surveillance equipment.
4. Encourage employee input on privacy issues.

"Team members" are more likely to adapt to privacy policies than "drone" workers.

On the collection and use of employee information:

1. Collect only the information necessary for a good decision. Explain to the employee why this information is necessary. Employee assistance program data should be kept separate and secure from any other employment data.
2. Information collected from employees is not to be shared in any capacity outside of the organization unless properly subpoenaed.
3. Employees should have access to their own personnel files and be able to question false information within them.

On drug and honesty testing:

1. Drug testing in cases of public safety is necessary. Other drug testing should be done only if employee behavior signals a problem.
2. Positive tests for drugs should be kept completely confidential and mandatory referral and successful completion of a certified drug education

program is required. Mandatory re-test in 180 days. Positive results require dismissal.

3. Written honesty tests should be used with discretion. Results alluding to dishonest behavior should be considered in conjunction with other factors such as criminal activity and not as the sole basis for employment.

On employee surveillance:

1. Employers may use surveillance of any sort at the business location, with the exception of designated employee rest areas, bathrooms, showers and lounges.

2. Employees should be instructed that company property and equipment are solely for the purpose of business use. Personal use is prohibited. A non-monitored pay phone should be provided for employees' use.

SELECTED BIBLIOGRAPHY

- "Don't Pry." The Economist 317 (1990): 18.
- Aalberts, Robert J., and Harvey W. Rubin. "Court's Ruling on Testing Crack Down on Drug Abuse." Risk Management 38 (1991): 36-40.
- Bahls, Jane E. "Checking Up on Workers." Nation's Business 78 (1990): 29-31.
- Bier, S.J., William C. Privacy: A Vanishing Value?. New York: Fordham University Press, 1980.
- Campbell, Duncan, and Connor, Steve. On the Record: Surveillance, Computers and Privacy - The Inside Story. London: Michael Joseph, 1986.
- Cappel, James J. "Closing the E-Mail Privacy Gap." Journal of Systems Management 44 (1993): 6-11.
- Carroll, Archie B. Business & Society: Ethics and Stakeholder Management. 2d ed. Cincinnati, Ohio: South-Western Publishing, 1993.
- Fitzpatrick, Robert B. "How to Avoid Invading Workers' Privacy." Business & Health 7 (1989): 14-6.
- Gray, George R., and Brown, Darrel R. "Issues in Drug Testing for the Private Sector." HR Focus 69 (1992): 15.
- Jacobs, Deborah L. "Are You Guilty of Electronic Trespassing?" Management Review 83 (1994): 21-5.
- _____. "The Perils of Policing Employees." Small Business Reports 83 (1994): 22-30.

- Katz, Lewis. Know Your Rights. Cleveland, Ohio: Brooks-Baldwin Law Publishing, 1993.
- Linowes, David F. Privacy in America: Is Your Private Life in the Public Eye?. Chicago: University of Illinois Press, 1989.
- Lissy, William E. "Workplace Privacy." Labor Law 54 (1993): 20-1.
- Mayer, Don. "Workplace Privacy and the Fourth Amendment: An End to Reasonable Expectations?" American Business Law Journal 29 (1992): 625-63.
- Parlman, Gregory C., and Erica L. Edwards. "Employee Assistance Programs: An Employer's Guide to Emerging Liability Issues." Employee Relations Law Journal 17 (1992): 593-601.
- Picard, Michele. "Working Under an Electronic Thumb." Training 31 (1994): 47-51.
- Rifkin, Glenn. "Privacy Matters." Harvard Business Review 72 (1994): 8-9.
- Schiller, Zachary, W. Konrad, and S. Anderson-Forest. "If You Light Up on Sunday, Don't Come In on Monday." Business Week (August 26, 1991): 68-70.
- Schoeman, Ferdinand D. Privacy and Social Freedom. New York: Cambridge University Press, 1992.
- _____. Philosophical Dimensions of Privacy: An Anthology. London: Cambridge University Press, 1984.
- Thornburg, Linda. "The High Cost of Delivering Data." HR Magazine 39 (1994): 49-52.
- Warner, David. "The Move to Curb Worker Monitoring." Nation's Business 81 (1993): 37-8.

Webster, George D. "Privacy in the Workplace." Association Management 43 (1991): 79-80.

_____. "Respecting Employee Privacy." Association Management 46 (1994): 142-3.

Young, John B. Privacy. New York: John Wiley & Sons, 1978.