

# 12

## **Workplace Privacy: The Social, Technical, and Ethical Ramifications**

Ryann MacDonald and Brendan Kroepsch

### **Introduction**

In the very near future, across the nation, hordes of students will be graduating from college. Before the last mortarboard floats to the ground, the final congratulatory toast is made, and the last grandparent gingerly boards a departing plane, the new graduates will be faced with many decisions about their future. Some decisions, like which sunscreen to use during a month-long sojourn in Spain, may not be pondered for very long. On the other hand, choosing between E.J. Gallo and Echo Star for a first job might require a pot of coffee and a family meeting.

Unfortunately, many young adults entering the work force do not have a firm understanding of the complex nature of the professional world. For these young people, the decision to take a job is routinely based on limited factors such as salary and medical insurance. Salary and benefits are imperative, but there are other regularly neglected questions that should always be posed to potential employers. For example, why is there an e-mail privacy disclaimer in my employment contract? Will my telephone conversations at work be monitored? Why is there a closed-circuit camera by the water cooler in the lunchroom? With respect to such questions about workplace privacy, a lack of experience can make young employees blind to the issues.

The purpose of this chapter is to help inform people about workplace privacy. Being more informed about workplace privacy issues will allow graduates to make sharpened social decisions and, hopefully, avoid any uncomfortable workplace privacy related situations in the future. The key issues to be addressed are: employee investigations, electronic employee surveillance, and legal privacy

protections. Each of the aforementioned sub-topics will be analyzed in-depth. Furthermore, at the end of the chapter, these issues will be dissected using widely supported ethical principles where applicable. After reading this chapter, some light will be shed on the controversial topics of the social, technical, and ethical ramifications of workplace privacy.

Privacy is a term often misinterpreted. The Supreme Court has broadly defined privacy as “the right of the individual to control the dissemination of information about oneself” (Rich 1995, par. 4). The definition of privacy as it applies to the workplace is based on the Supreme Court’s definition. However, three contingency tests must be applied on an individual basis to initially determine if an employee has an “expectation of privacy.” The three contingency tests are:

1. **A subjective test:** This test evaluates the means by which an employee has attempted to protect his/her privacy.
2. **An objective test:** This test evaluates the expectation of privacy an employee has in his office or desk in light of security measures and surveillance of employees in the workplace.
3. **A reasonableness standard:** This test judges whether the inception and the scope of invasion of privacy is reasonable under the circumstances... (Rich 1995, par. 6).

What does all this mean? It means that an employer has the majority of the decision making power as to whether the “dissemination” of personal information was done correctly or incorrectly, and if an individual should expect privacy in a given situation. “Our privacy rights on the job are much more limited than most of us believe” (Hubbart, 1998, p. 2). Do not expect to make an invasion of privacy claim and have it resolved easily. Simply defining workplace privacy is difficult, and defining it is only the first step in exploring workplace privacy issues. In today’s information age employee privacy expectations are constantly reduced. To protect personal privacy, every individual, from applicant to company veteran, needs to be wary of his or her surroundings. As William Hubbard states in his book, *The New Battle over Workplace Privacy*: “Privacy concerns begin at the start of the employment process” (3).

Workplace privacy with the sub-topic of employee investigations is at the forefront of this overview, specifically employment drug testing and background checks. The remaining portion of the overview will provide some fundamental knowledge about electronic employee surveillance (i.e., e-mail accounts and video surveillance) and what legal recourse, if any, are out there to protect the privacy of employees.

It definitely wasn’t a good idea for Joe to smoke a joint in Madrid during a graduation trip, especially when he discovers at the new job orientation the employer has a pre-employment drug testing policy. Now this presents some big questions. Who is required to take the test? Will he pass it? In the drug testing section of this chapter, this question will be addressed along with others. Furthermore, important consideration will be given to making ethical decisions concerning drug testing in the workplace today.

“Employee control methods have evolved drastically over the past few decades. Previous generations of workers were subject, for example, to having lunch boxes and purses searched or were forced to punch time cards” (Tunnell 2004). Today, searching through *your* peanut butter and jelly has turned into searching through the contents of *your* kidneys or even *your* scalp. According to Psychemedics Corporation (currently performing hair analysis for over 1,600 organizations), not only can the company detect the presence of a drug in a hair sample, but they can also provide accurate information on the quantity and history of drug use (Tunnell 2004). Before someone considers trying the latest super-hybrid drug in Europe, think of those people at Psychemedics, as “corporate drug testing policies have almost universally held up to challenges in court” (Maher 2004, p. B1). Background checks are another tool used by employers we will scrutinize.

Administering background checks has historically been more prominent within the government sector, but recently it has been utilized with increasing frequency in the public and private sectors. Companies, such as World Information Service of Tacoma, Washington, will provide clients with an applicant’s “address history, verification of Social Security number, criminal background checks, and driving history for \$80.” If additional information is deemed necessary, the same company can do a “civil check, credit report, and past employment verification for a mere \$45” (Rosenberg 1999, p. 8). Do people have any protection from prospective employers? Thankfully, workers do have some privacy rights in this area. Any company that is looking to hire must be careful with how it uses personal information in background checks because a number of state laws exist to cover ‘failure to protect confidentiality.’ Similarly, the use of e-mail accounts is coming under fire regarding the protection of private information.

In today’s modern business world, e-mail is a ubiquitous technology. “In 2000, 40 million employees exchanged more than 60 billion [e-mail] messages” (Griffaton and Porter 2003, p. 67). E-mail has drastically increased communication and business efficiency. From a negative perspective however, this increased efficiency has proliferated numerous privacy concerns. The nature of these concerns will be closely examined due to the fact that an increasing number of e-mail lawsuits have occurred lately. “The ePolicy Institute found that 60% [of employees] admitted to exchanging email that could be considered racist, sexist, or otherwise politically incorrect” (Griffaton and Porter 2003, p. 70). This study strongly supports the validity of the existence of employer/employee e-mail trust issues. In reality, e-mails should be thought of like postcards. When a postcard goes in the mail, anyone who cares to read it can.

To the casual observer, the business world is as open as a postcard thanks to the media who continually observe the business world, and reports to the public about the work environment in the United States. Whether it is a Dilbert cartoon in the newspaper or a disgruntled employee punching a computer on the news, these images make the workplace seem less and less inviting. Like the media watching the macrocosm of the business world, there is a new eye in the microcosm of the workplace called closed circuit television (CCTV).

In the video surveillance section of the chapter, readers will be given some answers as to why employers are installing closed circuit television cameras (CCTC). It is scary to think that CCTVs “can fit into a lamp, clock radio, briefcase, picture frame, utility pole, and other objects, and then they can be controlled remotely to pan, tilt, zoom and focus” (Rosenberg 1999, p. 9). Today it is almost impossible to know who is watching.

To the disadvantage of the employee, “local privacy laws vary from state to state and, like federal laws, are subject to judicial interpretation” (Hubbartt 1998). Some of the information in this chapter may come as a surprise, since the majority of the workforce has not paid much attention to workplace privacy issues. If more focus was given to these workplace privacy issues, perhaps fewer corporate lawsuits would be filed annually and there would be an increase in employee morale and performance. The ramifications of these issues run very deep. At the surface is employee drug testing.

### **Employee Drug Testing**

It has only been within the past 20 years that drug use has been defined as a social problem by science professionals and, more importantly, employers. According to Kenneth D. Tunnell, from 1981 to 2000 the public expenditure to combat drug use in the United States rose from \$1.5 billion to \$19.2 billion (1). That is an overall increase of 1200%. Needless to say, addressing drug use in American society is a great financial priority.

The highest priority of most young adults graduating from college is to find a job and become financially independent. However, with greater competition for a limited number of positions and a many pre-employment tests to pass, young people are finding it harder and harder to secure a desirable first job. One employee test consistently administered today is drug testing. Within the chapter overview, this question was posed: Should young adults entering the workforce, who have recently “experimented” with drugs, be worried? The simple answer is yes. “Pre-employment screening currently is the most commonly used type of drug testing. 78% of companies require job-applicant drug testing” (Tunnell 2004). Lockheed Martin, one of Colorado’s largest employers, is just one of the companies that comprise the 78% figure. In a small survey conducted for this chapter, 58% of the respondents strongly agreed that employee drug testing increases company performance. On the other hand, 16% strongly disagreed. Interestingly, within this study, 100% of the Lockheed Martin employees surveyed strongly agreed that drug testing increases company performance. This probably has to do with the fact that all prospective Lockheed Martin employees are required to take a pre-employment drug test. Another finding worth noting is the fact that the average score (on a 7 point scale with 7 being “strongly disagree”) for the question, “I am concerned about workplace privacy” was a 5 for the Lockheed Martin employees, indicating that they are not concerned with privacy issues. Lockheed Martin is an aerospace engineering juggernaut. It has offices all around the globe. Could it be possible that large companies are going to require drug testing on a more consistent

basis than small companies? For a young person attempting to obtain a job, this could be a very important question in the employment search.

Viewing business from a sociological standpoint would reveal that larger businesses are more likely to drug test than small businesses. "Drug testing is far likelier within large, heterogeneous organizations characterized by distant social relations" (Tunnell on Black 2004, p. 103). On the other hand, people working in small organizations are able to interact with more levels of the organization and, at the same time, build a positive reputation and higher level of trust amongst their peers. Often, the only time an employee will be drug tested, in a small firm, is if a pattern of misconduct arises. On a basic level, "drug testing, as surveillance, is a relatively easy solution for employers who have few methods available for distinguishing reputable from disreputable individuals" (Tunnell 2004). The question of reputability is one a large company has a very limited history with concerning any new applicant. Thus, tools like drug testing might be the best option for a large firm to avoid making hiring mistakes.

Drug testing is an employment instrument that is not going to disappear in the near future. America's society has defined drug use as a problem and continually supports increases in the financial funds available to fight "the war on drugs."

### **Employee Background Checks**

Security and liability concerns that have recently arisen make it necessary for many employers to conduct background checks on applicants. Background checks are said to protect a company from hiring an applicant that may be prone to injuring others. Employers may also conduct background checks for purposes of ensuring applicant quality control. Accordingly, 64% of employers frequently conduct credit checks, 56% verify driving record, and 61% investigate applicants' criminal records. In a recent Society for Human Resource Management (SHRM) survey of 1,000 employers, "69% administered some sort of background check on all potential employees" (SHRM / West Group 2000, p. 9). However, employers cannot get any information they wish to about their prospective employees (although it may be available). They must be careful. Seeking information about an applicant's personal life that is irrelevant to job performance may expose the company to a privacy lawsuit from the applicant. Employers are also responsible for ensuring that all information obtained during the investigation is held in strict confidence and only divulged to those who absolutely need to know, such as personnel in human resources and those involved with making hiring decisions.

Background checks involving previous criminal convictions are allowed. However, it is illegal in many states to request information regarding past arrests and drug treatments (since a guilty verdict may not have been reached). It is legal for an employer to reject an applicant who is a convicted felon, as long as the "conviction is related to job duties" such as a convicted shoplifter who applies for a position in retail (Shumaker 2002, p. 31). Employers may ask employees if they possess the physical capacity to perform as long as it is job related, such as UPS workers who have to lift heavy packages, but investigating past workers compensation claim and medical history is off-limits. If an

individual is applying for a position that involves the handling money, a background check into their credit may be appropriate. This will help protect the company's assets and identify individuals who might be prone to stealing, such as "an applicant deep in debt who might be tempted to siphon [company] money to pay off credit cards" (Shumaker 2002, p. 31). Failure to hire or promote an employee based on an unsatisfactory credit report is acceptable but the person must receive a copy of this report.

Background checks may feel like just another invasion of privacy in the workplace. But before someone decides to refuse an employment background check, it would be wise look at the situation from the point of view of the prospective employer. Choosing an employee has large long-term impacts on an organization that could be positive or negative. When a person should be concerned is when an employer is checking background information that has nothing to do with the direct responsibilities of a position. Once someone finally manages to find a good job, there are still many privacy issues within the company to deal with, like video surveillance.

### **Employee Surveillance: E-Mail and Video**

Since the introduction of the Internet and e-mail into the workplace, business and communications have become quicker and more efficient. Now, employers who were once praising its capabilities are voicing concerns over how this technology is being used by their employees. In a study recently conducted by Yankelovich Partners, 62% of employees admitted to using the Internet for personal use on a daily basis, and 44% use their company e-mail account for both work and personal purposes (Whitney 2003, p. 20). With such a high occurrence rate, employers "must protect against the actions of employees who download pornography or copyrighted music, send harassing e-mail, reveal company secrets, disclose personal information, or sell drugs" (Greenwald 2004, p. 1). Additionally, they want monitoring capabilities to help measure performance and productivity. One study showed that "80% of employers reportedly monitor e-mail and an additional 76% monitor employee computer usage;" (SHRM / West Group 2000, p. 8) thus, resulting in "the single greatest invasion of any sensible space of privacy that cyberspace has produced is the extraordinary monitoring of employees in which corporations now engage" (Frayer 2002, p. 858).

Employers are able, with the help of such product like the Silent Watcher by Adavi Inc., to "track the amount of computer idle time of each worker, record every keystroke made, create and e-mail to a designated person, create a log of every Internet site visited, and monitor all incoming and outgoing e-mail" (Frayer 2002, p. 858). They can even view the activities of employees in real time. In some instances, employers can determine which sites are being visited most frequently and then have the system block employee access to these sites. The system can be customized to allow employees to view these sites during their lunch hours but, for the most part, employers want to discourage such distractions as much as possible. For liability purpose, most companies also store and make back-up copies of all material sent over the Internet. However, they must be careful that they do not store

the information for too long or even too short of a time. Over the long-term, these massive amounts of files can “strain storage and management resources, as well as preserve smoking guns” (Chudnow 2003, p. 1). On the other hand, getting rid of these files too quickly might “violate regulatory laws and invites litigation” (Chudnow 2003, p. 1). Another form of monitoring used by employers that may invade privacy is video surveillance via Closed Circuit Television (CCTV).

Employers hope videotaping employees as they go about their daily activities, will promote a more productive and safe work environment. Over 34% of employers who responded to the 2000 Workplace Privacy Survey said that they have installed video surveillance equipment in the office (SHRM / West Group 2000, p. 14). This is up from 11.2% in 1991. In some cases, the presence of CCTV has been proven to discourage physical confrontations, sexual harassment, and stealing, but employees are often wary of how footage of them is actually used. Workers are concerned about privacy violations and the use of the technology for purposes other than those originally intended. It certainly increases overall stress and mistrust, and negatively affects morale. So the most important question is, do the pros of CCTV outweigh the cons? Is this electronic monitoring with e-mails and CCTV fair? Are any of the workplace privacy issues discussed up to this point fair and/or legal? The next section’s goal is to look at the legal side of workplace privacy issues.

### **Workplace Privacy Laws**

Due to the dynamic nature of technology and the apparent necessity of employers to monitor their employees’ every move, new conflicts within the workplace have formed between the two groups. These problems are unique since technological advances are constantly changing the nature of the work environment and modes of communication. As technologies advance, employees are seeing an increasing propensity for employers to take actions that limit their privacy. Laws governing and protecting privacy in the workplace are emerging, but they aren’t keeping pace with technology.

More and more, employees believe that employers are abusing their power by invading their privacy. Approximately 5% of all companies in the United States have been brought to court concerning issues of e-mail privacy violations in the workplace. Another 14% have been required to produce e-mail records and e-mail accounts by courts or investigative agencies (Whitney 2003, p. 20). There are laws that exist to protect employees, beginning with the Fourth Amendment to the Constitution. The Fourth Amendment protects Americans from unreasonable searches and seizures but has been extended to incorporate workplace situations, such as “the involuntary administration of drug tests and protection from employer intrusion into personal papers” (Cozzetto 1997, p. 516). In regards to electronic communications, if an employee has a reasonable expectation of privacy then employers cannot monitor their Internet, phone, and fax activities. This applies only to publicly employed individuals, such as government workers and some government contractors. In addition, 24 states, including Colorado, protect the individuals’ right to privacy through state constitutional provisions or statutes. Some of these constitutional

provisions or statutes have been held to create a civil claim for invasion of privacy by private parties, while others have not. Probably the most groundbreaking government legislation dealing with workplace privacy protections is the Electronic Communications Privacy Act (ECPA) of 1986.

The ECPA of 1986 prohibits employers from intercepting e-mails, telephone calls, and faxes. Its intent is to "update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies," and is the only piece of federal legislation that addresses e-monitoring (Sproule 2002, p. 66). Major exceptions to this law, where employees would not be protected, occur during instances where the employer maintains the system, the employee consents to being monitored, or the employer has a legitimate business purpose for the surveillance (called the "business-use exception"). Therefore, authorized co-workers, supervisors, and system administrators would have access to all internal information passed, without liability. The Wiretap Act prohibits employers from "intercepting and recording the 'wire communications' of employees" (Cozzetto 1997, p. 518). The actual conversation that transpires is protected and extends to audio equipment, so CCTVs with audio capabilities may violate this act.

Another privacy issue relates to the disclosure of medical information. The Health Information Portability and Accountability Act (HIPAA) "sets forth specific requirements relating to confidentiality and privacy of medical records and medical information" in limited and specific circumstances (Whitney 2003, p.23). For instance, medical information that is collected for managing insurance must be held in strict confidence and protected with the necessary security such as encryption, firewalls and passwords. Aside from legal protection within the workplace, many laws also exist that protect applicants during the hiring process.

In accordance with the Fair Credit Reporting Act (FCRA), employers must gain the consent of the employee whom they wish to conduct a background check. After consent is obtained, employers will then have access to a plethora of information ranging from driving records to credit history or even interview past associates and family members. An applicant is not required to submit, but will likely forfeit any chance of employment if he or she chooses not to. Many employers also request that the applicant take a drug test. Failing to do so will also result in not being hired.

Applicants can seek protection under the Americans with Disabilities Act (ADA) if they are probed about past treatment for a drug problem during the interview process. Not only can an employer not ask the potential employee about this information, but they also cannot conduct a background check to expose past treatment records. Employers can, however, obtain any information relating to current drug use.

The answer to the question "Do I have any legal privacy protections?" is yes, but with certain restrictions. There have been some improvements in regards to protecting personal information through the ECPA, HIPAA, and other government doctrines but the privacy legislation landscape is very fragmented. "...Although a number of

independent laws and acts have been implemented over time, no single overarching national data privacy policy has been developed. As a result, existing legislation is sometimes inconsistent and even conflicting at times" (Reynolds 2003). After analyzing the workplace privacy issues of this chapter, it is now time to evaluate them from another very important perspective: ethics.

### **Ethical Analysis of Workplace Privacy**

Marvin Bower, a former managing partner of McKinsey and Company, once said, "There is no such thing as business ethics." He continues with, "there is only one kind: you have to adhere to the highest standards" ("Advice on Business Ethics," 2004, par. 1). Unfortunately, adhering to the highest standards, ethically, is not something that all businesses do. Many companies and individuals within them often believe that the only reason a company exists is to make a profit. Continuing with this thought, Ralph Clark and Alice Lattal, authors of *Workplace Ethics: Winning the Integrity Revolution*, pose an intriguing question. They ask, "In other areas of life no one lives by a single value [so] why should business be [the] exception?" (25)

When one looks out across the vast business landscape, "exceptions" seem to be the rule when dealing with ethics. A very basic and widely accepted perspective is that, "sometimes, the [ethical] rules do not seem to cover new situations, and you must determine how to apply the existing rules or develop new ones" (Reynolds 2003). Thankfully, many businesses and places of higher education, like the Leeds School of Business at the University of Colorado at Boulder, are doing exactly this:

The Leeds School recently launched the Center for Business and Society. The Center spearheads the school's business and society initiatives that provide a broad approach to business education. The Center also supports and encourages intellectual inquiry into the role of business in society, including business ethics and leadership, as well as the impact of business on the environment ("About the Center," 2004, par. 1).

Business students across the nation are now realizing how important ethics are and that business is much more than making a profit. Many different scholars have outlined their reasons why firms, large and small, need to promote ethics. Some of these theories overlap, but the cardinal ones are "to protect the organization and its employees from legal action, to avoid unfavorable publicity, and to gain the goodwill of the community" (Reynolds 2003). It is a sensitive business objective to promote ethics. Furthermore, firms face an even greater challenge drafting ethical codes and then enforcing them. Making sound ethical decisions requires, at a minimum, "getting the facts, determining the stakeholders, considering consequences of decisions, weighing various ethical principles, and reviewing [one's] decision" (Reynolds 2003). Elements of this basic ethical framework will be implemented at the onset of this section for the purpose of more accurately understanding the dynamic process of ethical decision-making as it pertains to issues in workplace privacy.

Whether someone is a prospective employee or a company veteran, employee drug testing is highly controversial and has enormous ethical ramifications. Lockheed Martin has to make ethical decisions regarding employment and drug use everyday. The facts are as follows: John Doe, 23 years old, is applying to work at Lockheed Martin, and has recently smoked one joint at a college party. The stakeholders are John Doe and Lockheed Martin Corporation. What are the consequences of smoking that joint? Either John will not be hired, or Lockheed Martin will hire John, based on passing his drug test. The result of John being hired is that he might create future problems in the company due to his sporadic drug use. One of the hardest parts of reviewing ethical situations is evaluating and applying ethical principles.

In this situation, the most logical ethical approach is that of the utilitarian. With this approach, the best ethical choice is the one that “produces the greatest excess of benefits over harm” (Reynolds 2003). Employers utilize drug testing to protect the workplace community as a whole, creating the greatest benefit. Will John Doe negatively affect the Lockheed Martin workplace and decrease productivity if he occasionally smokes pot? The bottom line is that if John doesn’t pass his drug test, he will not get the job because Lockheed Martin is ethically consistent when it comes to drug testing. This is a black and white decision if John fails his drug test. However, if John passes his test, the whole ethical situation will have to be re-evaluated using the steps just completed. The only definite in ethics and ethical decision-making is that it is a dynamic process.

Evaluating drug testing is just as ethically dynamic as evaluating background checks. Background checks, for employment purposes, are becoming extremely easy to perform and are being employed on a wider scale. A large number of college seniors applying for jobs have to sign paperwork that will allow a prospective employer to complete a background check. There are companies that will complete background checks for a small fee of around \$45.

The ethical principle that applies most directly to background checks is the common-good approach. This ethical choice is one that “advances the common good” (Reynolds 2003). It could be stated that background checks on potential employees are performed to advance the common good of the businesses they hope to join. Realistically, the ethical decisions pertaining to background checks fall more squarely on the shoulders of an employer than the employee, since it is the employer that is accessing potentially sensitive information. When employers access personal employee information, they need to use strict methodology for processing the information and coming to an ethical employment decision. Once again, the idea of ethical consistency is raised. If employment decisions are made based on background information and are consistent across all situations, fewer problems will arise. It should be stressed that company ethics policies are very powerful decision-making tools. In fact, “although only 21% of the [ethical] policies in existence in 1987 showed board involvement, participation had increased to 41% in 1991 and to 78% by 2000. Gaining the attention of the board of directors shows that an increased level of importance is placed on ethical standards” (Reynolds 2003). Similarly,

privacy policies regarding employee monitoring and ethical decision-making are also very important in today's business world.

"Currently, 78% of major United States firms find it necessary to record and review employee communications and activities on the job, including phone calls, email, Internet connections, and computer files." (Reynolds 2003). This is an important statistic as it relates to workplace privacy and ethical considerations. When it comes to electronic employee surveillance, a solid basis for incorporating sound ethical decision-making would be the fairness approach rather than using the utilitarian or common good approach. The fairness approach is the ethical choice "that treats everyone the same and does not show favoritism or discrimination" (Reynolds 2003). Logically, if a firm implements employee monitoring through e-mail and video surveillance, every employee should be subject to the monitoring. A company should not be able to play favorites and only monitor a certain population of its workers.

If an invasion of privacy claim is made, an employer should be able to support its arguments about monitoring with a clear privacy policy and a monitoring agenda that encompasses all employees. This point was partially supported by our workplace privacy survey in the realm of video surveillance. After reviewing the data collected, it was discovered that 100% of the respondents were subject to video surveillance and were aware of its presence in the workplace. The results pertaining to e-mail monitoring were not as statistically strong, but were quite interesting. Thirty-three percent of those surveyed did not know if their company had an e-mail privacy policy. A recommendation to the employers of those surveyed would be to communicate its policies in a stronger manner or create a privacy policy if it doesn't exist.

### **Conclusion**

"Since 9/11, employees have shown a willingness to surrender some of their privacy for the sake of security. However, as employees begin to get comfortable and feel safer, the issue of privacy protection will re-emerge. It now becomes important for employers to develop a clearly written and comprehensive privacy policy that defines what is considered company property" (Sproule 2002, p. 68). According to the 2000 Workplace Privacy Survey, 75% of respondents "believed that their organization's written formal policies have played an important role in preventing privacy related lawsuits and disputes" (SHRM / West Group 2000, p. 9). Privacy policies are used to protect the company from legal liability, security concerns (protecting corporate assets), legal compliance, and are a method to evaluate employee performance and productivity. This policy should cover employee/employer rights, security issues, as well as consequences for failing to comply. It should also clearly state when and in what specific circumstances an employer can conduct searches. While drafting and distributing the policy to employees, it is important for employers to remain sensitive to employees' private interests. The policy should be signed by all employees upon their acceptance of employment as an acknowledgement that they have read and understood all of its provisions. Employers should also redistribute copies of the privacy

policy each year and highlight its amendments. Employees should understand that the purpose of privacy policies is not to hurt them, but to protect them within their workspace.

With knowledge comes power. Individuals have the right to know which privacy rights they are giving up when accepting a job. They also have the right to be protected against any privacy violations by employers. Don't forget, someone is always watching. Be careful.

### Works Cited

- Chudnow, Christine Taylor. "Business Dilemma: E-Mail Retention Policy." *Computer Technology Review*. Los Angeles: Jan 2003. Vol. 23, Iss. 1, p. 1.
- Clark, Ralph W. and Lattal, Alice D. *Workplace Ethics Winning the Integrity Revolution*. Rowman and Littlefield Publishers: Lanham, 1993.
- Cozzetto, Dan A. and Pedeliski, Theodore B. "Privacy and the Workplace: Technology and Public Employment." *Public Personnel Management*. Washington: Winter 1997. Vol. 26, Iss. 4, p. 515-527.
- Frayner, Charles E. "Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests." *The Business Lawyer*. Chicago: Feb 2002. Vol.57, Iss. 2, p. 857-874.
- Greenwald, Judy. "Privacy Issues Creating Dilemma for Employers." *Business Insurance*. Chicago: Feb. 16, 2004. Vol. 38, Iss. 7, p. 1-2.
- Griffaton, Michael C and Porter, William G. "Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace." *Defense Counsel Journal*. Chicago: Jan 2003. Vol. 70, Iss.1, p. 65-77.
- Hubbarrt, William S. *The New Battle Over Workplace Privacy: How Far Can Management Go?*, American Management Association (Amacom): New York, 1998.
- Maier, Kris. "Armchair Drug Detection: Devices Sweep Office Fixtures For Illegal Substance Traces; Viewed as 'Kind of Sneaky.'" *Wall Street Journal* (Eastern Edition). New York, N.Y.: Jan 20, 2004. p. B1.
- Reynolds, George. *Ethics in Information Technology*. Thompson Publishing-Technology Division: Boston, 2003.
- Rich, Loyd L. "Right to Privacy in the Workplace in the Information Age." The Publishing Law Center. 1995. <<http://www.publaw.com/privacy.html>> (12 Oct. 2004).
- Rosenberg, Richard S. "The Workplace on the Verge of the 21st Century." *Journal of Business Ethics*. Dordrecht: Oct 1999. Vol. 22, Iss. 1, Part 2, p. 3-14.
- SHRM / West Group. "2000 Workplace Privacy Survey." *Society of Human Resource Management Research*. 2000, p. 8-14.
- Shumaker, Thomas A. "An Employee Privacy Policy Fairly Applied Can Prevent Privacy Litigation." *The National Public Accountant*. Washington: Apr / May 2002. p. 31-33.
- Sproule, Clare M. "The Effect of the USA Patriot Act on Workplace Privacy." *Cornell Hotel and Restaurant Administration Quarterly*. Ithaca: Oct 2002. Vol. 43, Iss.5, p. 65-73.

- Tunnell, Kenneth D. "Pissing on Demand." New York University Press: New York, 2004.
- Whitney, Jo Ellen. "Taming the Monster: Employee Privacy and the Law." *Rural Telecommunications*. Washington: Sep / Oct 2003. Vol. 22, Iss. 5, p. 20-24.
- "Advice on Business Ethics. Quotes Quotations." AdviceonManagement.com. 2004. <[http://www.adviceonmanagement.com/advice\\_ethics.html](http://www.adviceonmanagement.com/advice_ethics.html)> (20 Oct. 2004)
- "About the Center." Business and Society Center, Leeds School of Business at the University of Colorado at Boulder. 2004. <<http://www.leeds.colorado.edu>> (23 Oct. 2004)