

SHRM

WHITE

PAPER

WORKPLACE PRIVACY: WHOSE RIGHT IS IT?

By Christine V. Walters, MAS, J.D., SPHR, and Merry Lee Lison, SPHR

August 2005

Introduction

As technologies advance, so do the complexities of balancing the employer's need to protect its assets and provide a safe workplace with a respect for employees' privacy. Some of the more intriguing workplace privacy issues involve the use of implantable "verichips" used to verify employee access to highly secured areas or information;¹ biometric time clocks that scan fingerprints;² and global positioning systems or GPS tracking devices.³

Employers are all too aware of these issues and the challenges they present. The *SHRM/West Group 2000 Workplace Privacy Survey* reported that approximately 75% of survey respondents indicated that they always or sometimes monitored employees' use of Internet, 63% monitored e-mail activity and 40% monitored telephone calls. So common are various forms of workplace monitoring of employee activity that *WIRED* magazine published "Ranking Privacy at Work"⁴ in 2003 and 2004 and there was an international conference on HR privacy held in Washington, D.C.

This paper is written to provide HR practitioners and business owners with some proactive considerations for protecting the employer's assets, providing a safe workplace and respecting employees' privacy.

Searches

Workplace-based searches raise a variety of questions and have numerous implications. What is to be searched on a person or property? Whose property and why? Who will conduct the search? Is it a private or public employer? The answers to these questions, along with additional considerations,

determine the best way to proceed in any given situation.

Public Sector

Two provisions of the Fourth Amendment to the U.S. Constitution limit government action and protect citizens' privacy rights. This includes citizens when they are government or public-sector employees. Those provisions are extended to state and local governments through the 14th Amendment. This constitutional right to privacy does not apply to employees in the private sector. When does the government as the employer have the right to search an employee, employee's property, possessions or workspace without violating the employee's reasonable expectation of privacy under the Fourth Amendment? It depends upon the facts, circumstances and answers provided to the questions in the above paragraph.

In *O'Conner v. Ortega*, the U.S. Supreme Court ruled that the very nature of a public employee's position allows some intrusions into privacy that would not otherwise be tolerated by the Fourth Amendment. In that case, state hospital managers placed a physician on administrative leave pending an investigation of alleged improprieties. During the investigation, the managers searched and obtained certain evidence from the physician's desk and filing cabinets that was used as a basis for his subsequent discharge. The Court upheld the search because it was based on a reasonable suspicion that the search would turn up evidence that the employee was guilty of work-related misconduct. The search of an employee's property, such as an employee's briefcase, purse or wallet, is given closer scrutiny and will generally require a warrant prior to search. Some courts, however, have upheld such searches as in the case of an employee who was suspected of concealing child pornography in a storage unit in her office, which she had purchased at her own expense and for which only she had the key.

Private Sector

Private employers have more leeway in conducting searches, although there are still privacy considerations under common law as well as some state laws that have created workplace privacy rights. A number of states have passed legislation granting specific privacy rights to employees and placing obligations upon employers, especially with regard to electronic monitoring. So when may a private employer properly conduct a workplace search? A key to answering this question is closely tied to the issue of whether the employee had a reasonable expectation of privacy in the item that was searched and the employer's legitimate, business reason for conducting the search. For example, take the case of an employee who is provided with a locker at work. The employee is permitted to use his or her own lock and is not required to provide the combination to that lock to his or her employer. There is no policy regarding searches. Does the employer violate the employee's privacy when it breaks the lock and searches the employee's locker without his or her consent? One Texas jury answered "Yes" to the tune of a \$108,000 award to the employee.

In addition, private employers need to safeguard against common law claims, including invasion of privacy, unreasonable intrusion upon the seclusion of another, unreasonable disclosure of personal facts, false light publicity, seclusion, outrageous conduct, intentional infliction of emotional distress and more. Managers and supervisors should be reminded not to disclose personal employee information to staff and co-workers, even with the best of intentions. Take the case of employees who asked about their co-worker who had been absent for some time. In response to their concern, the supervisor

disclosed that the employee had a mastectomy. The employees then took up a collection and sent flowers and a get-well card to the employee's home. When the employee received the flowers, she was mortified that the supervisor had disclosed such personal information to her co-workers. She subsequently sued and won.

Employer Access to Employee Information

In the course of employment, companies need access to some personal information regarding its employees. Various federal, state and common laws address the collection, retention and disclosure of this information.

Employment Files and Records

Protecting the privacy of personal data in the employment setting is a hot topic now, but by no means is it a new one. For example, the Federal Privacy Act (USC 552a), which regulates access to information contained in government records, has been in existence since 1974.

Protecting the privacy of employees' personal information goes beyond adhering to legal recordkeeping requirements. HR professionals should create procedures to make sure only necessary information is maintained and that it is properly disclosed.

To decrease the risk of invasion of employee privacy claims, employers should:

- 1) Only collect and maintain private information that is reasonably necessary for business purposes.
- 2) Not release information without the employee's consent nor disclose it to parties that do not have a need to know.
- 3) Ensure information that is disclosed is accurate.⁵

Employee Medical Information

When the private information is related to the employee's health or medical conditions, there are several federal laws the employer needs to be mindful of. A brief description on how each of these affect employee privacy follows.

Family and Medical Leave Act of 1993: Medical information gathered for leave purposes must be kept confidential and can not be maintained with other personnel information. The employee must authorize his or her health care provider to release information to the employer.

Occupational Safety and Health Act of 1972: The names of employees injured by objects tainted by potential blood-borne pathogens cannot be disclosed. Employers are required to use "privacy case" instead of the name in these cases and for several other types of cases described in 29 CFR §1904.29, 1910.103(h).

Americans With Disabilities Act of 1990: Obtaining, using and maintaining information about an employee's medical conditions must adhere to certain restrictions. Like the Family and Medical Leave Act, this Act also requires that medical information be kept confidential and maintained separate from other personnel information.

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules: The privacy rules are the most recent and probably most complex of the legal restrictions on employee medical information. Employer-sponsored group health plans, not the employer, are covered by these rules.

The health plan must limit access to an employees' protected health information (PHI) and ensure it is not used in employment-related decisions. The rules specify permitted uses and disclosures of PHI and require that staff members who have access to this information be trained regarding privacy rules. It also specifies that plan participants' rights and correction and complaint mechanisms are communicated.

The rules state that PHI does not include employment records gathered only for the purpose of implementing the employers' business practices or legal duties such as workers' compensation records. In these cases, it is not the information contained in the record but rather the purpose for which the record will be used that determines which regulation must be adhered to.

Additional HIPAA Privacy legislation went into effect in 2005. This part of HIPAA addresses security standards that ban improper access to or alteration of PHI.

State Laws Regarding Employee Information

Many states provide similar employee information protections to those mentioned above. Some have laws specific to disclosing or accessing employee records.

Certain states limit the release of information to third parties, such as for reference checks conducted by prospective employers. In some cases, certain types of information cannot be disclosed without advance written approval from the employee.

Regarding employees' access to their own personnel records, state laws vary greatly. Some statutes are quite general and allow access to any record while others limit access to very specific types of documents. Records that are frequently off limits to employees include test materials, reference letters, criminal or civil investigation documentation and operational planning information.

Invasion of Privacy Claims

Although there are no federal laws that prohibit privacy invasion in the private employment sector, state laws do provide some protection for a reasonable expectation of privacy to individuals.

To assess if an invasion of privacy claim has validity, the courts view an employer's collection and use of information about the employee and determine if the employee was harmed by the disclosure. If the claim is valid, the employer could be liable for damages for harming the employee's reputation or

causing mental stress, in addition to punitive damages.

To protect themselves from invasion of privacy claims, employers should clearly define their rules and expectations regarding workplace privacy in their company policies. Having safeguards in place to prevent unauthorized access to information is another good defense to an invasion of privacy claim.⁶

Identity Theft

In light of increased identity theft, the government is responding to concerns about protecting the privacy of Social Security Numbers (SSN).

On July 21, 2004, the House Committee on Ways and Means approved H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2004. The bill would restrict “the sale, purchase and display of SSN in the public and private sectors; provide additional measures to protect SSN privacy; help ensure SSN are assigned accurately and create criminal and monetary penalties for persons who misuse SSN.”⁷

At the state level, nearly a dozen states have laws protecting the privacy of SSN. Some specify restrictions for putting SSN on documents, Web pages or materials that are mailed to employees’ homes. It is likely that more states will be addressing SSN privacy in the near future.

Identity theft is a growing concern for employers not just because it is disruptive and decreases the productivity of affected employees, but also because much of the theft is occurring in the workplace. According to a September 2002 report by one of the largest credit bureaus in the nation, TransUnion, “the number one underlying source of identity fraud is theft of employer records.”

To avoid liability for identity theft, employers should take every precaution to protect employee records by storing files in locked cabinets, having appropriate levels of security to access electronic data and thoroughly investigating the backgrounds of employees who have access to this data.

Having a plan in place to respond to identity theft if it occurs is also important. Some companies have even gone to the point of offering their employees a benefit that provides protection, recovery and reimbursement from identity theft.⁸

Investigative Inquiries

Employers may have a valid business interest along various stages of the employment relationship in seeking information about current or prospective employees. The employer’s rights and duties vary depending upon what information is obtained and by whom.

Background Checks and Investigative Reports

In the SHRM/West Group study, 69% of respondents indicated that their companies conducted some form of a background check on employees. Most used a third-party vendor to provide these reports. Some used vendors to verify prior employment, education and more. In this case, the federal Fair Credit Reporting Act (FCRA) requires certain notices be provided to applicants and employees for whom the

employer is obtaining a consumer report or investigative consumer report.

*The FCRA, Consumer Reports and Investigative Consumer Reports*⁹

The FCRA applies when an employer obtains certain reports on an individual that are obtained through a third-party vendor who is a consumer reporting agency (CRA). A consumer reporting agency is a vendor or entity that is in the business of regularly supplying these types of reports. Consumer reports include “any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which [may] be used...as a factor in establishing the consumer’s eligibility.” Examples of such reports would include credit, criminal history or driving record.

Investigative consumer reports are those “in which information on a consumer’s character, general reputation, personal characteristics or mode of living is obtained through personal interviews with neighbors, friends or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information.”

For example, if the employer calls and interviews personal references or previous employers that the applicant provided, that information is not covered under the FCRA. However, if the employer contracts with a vendor and the vendor obtains the same information through personal interviews, then that information would constitute an “investigative consumer report” and would be covered under the FCRA.

What difference does it make whether you have requested a consumer report or an investigative consumer report? The notices required and the timing of the notices vary depending on the type of report being ordered.

Required Notices

The FCRA requires four notices for consumer reports. The first is between the CRA and the employer notifying the employer as a user of a consumer report or consumer investigative report, including the employer’s duty to comply with the FCRA.¹⁰ The second is a notice and authorization form provided by the employer to the employee or applicant. This authorization must be obtained prior to requesting the report from a CRA, but it may be obtained far in advance. For example, an employer may have all applicants sign a document that authorizes the ordering of a consumer report at any time before or during the individual’s employment with the company, if the individual is hired. The third notice is a pre-adverse action notice. If information obtained through the report causes the employer to take some adverse employment action (not hiring an applicant, taking corrective action or terminating an employee), the employer must first provide the applicant or employee with an adverse action notice. This notice must contain certain specific information and be provided to the applicant or employee, along with the FTC’s prescribed “Summary of Your Rights Under the Fair Credit Reporting Act”¹¹ and a reasonable period of time for the employee or applicant to inform the employer if the report is inaccurate. Finally, if the employee decides to proceed with the adverse employment action, the employer must then send the employee or applicant an adverse action notice. This again must contain

some specific information.

The employer's notice requirements for investigative consumer reports are the same as for consumer reports, with the exception of the notice and authorization. The notice and authorization may be obtained after the report is actually ordered, but not later than three days after the report is ordered. Thus, an authorization form signed prior to or upon employment will not suffice should the employer want to obtain an investigation consumer report later in the employment relationship. A new authorization would have to be obtained. Once notified that an investigative consumer report has been ordered, the individual then has the right to request additional information regarding the nature and scope of the investigative consumer report, and the employer must fulfill this request.

But what if the employer is seeking a report as part of an investigation related to suspected workplace misconduct? In December 2003, President Bush signed the Fair and Accurate Credit Transactions Act (FACT) which reauthorized and amended the FCRA. FACT, which became effective in March 2004, excludes from the definition of "covered reports" communications that are "made to an employer in connection with an investigation of suspected misconduct relating to employment." In this case, no authorization is required. If the employer decides to take adverse employment action based on information in the report, the employer is then obligated to disclose to the employee a summary containing the nature and substance of the report. Note that credit reports are not covered in this exclusion.

Investigating Off-Duty Conduct

When does the employer have the right to investigate an employee's off-duty conduct or take adverse employment action based upon such conduct? The answer once again is it depends. Generally speaking, the employer must be able to demonstrate good faith and a legitimate business reason for taking such action.

Unauthorized Use of Computers and Cell Phone Cameras in the Workplace

Monitoring for unauthorized use of computers and the Internet in the workplace is a widely debated issue.

Employers seek to balance the need for security while respecting employees' privacy. Shanti Atkins of Employment Law Learning Technology describes it this way: "Corporations are really in a bind. They can be sued for either violating an employee's privacy by exercising too much control over electronic communication or Internet use, but also for not exercising enough control and allowing workers to be subjected to harassment."

A policy forbidding personal computer and Internet use in the workplace is not realistic because it is generally unenforceable. However, having no policy potentially sets the stage for invasion of privacy claims and makes the employer liable for employees' inappropriate use of e-mail and other systems.

Discrimination, harassment claims and copyright infringement are just a few examples of situations where companies can be unwittingly liable for employees' behavior if they don't monitor computer and

Internet use.

As mentioned previously, no federal law exists to protect workplace invasion of privacy, and at the state level, right to privacy is based on a “reasonable expectation of privacy”. However, attorney Michael Overly, author of *E-Policy: How to Develop Computer, E-Policy and Internet Guidelines to Protect Your Company and Its Assets*, notes that the courts have said if a company has a written policy notifying employees of computer and Internet use monitoring, the expectation of privacy is removed.

There are other technology issues that could cause an employee’s privacy to be violated that fall outside of monitoring computer activity.

Not removing sensitive data before disposing of computer hard drives could create legal issues for employers. Many people take for granted that organizations are properly discarding equipment, but it’s not happening, according to Bob Knowles, president of Technology Recycling. He predicts more invasion of privacy claims to arise from sensitive information being left on discarded hard drives.

Cell phones with digital cameras are another technology advancement that can create problems for employers. The potential to use the phone for voyeuristic purposes, such as secretly filming co-workers in the employee changing area and then sending the pictures over the Internet, has become a growing concern.

Similar to having a policy banning all personal use of computer equipment, a policy of banning phones is probably not enforceable. However, Joanna Krotz of Muse2Muse suggests that a workable policy may be to restrict the use of camera phones for private pleasure while being paid by the employer. She further recommends posting notices to prohibit camera cell phones in private areas such as bathrooms and changing areas.

Even though employees’ expectations for privacy in the workplace should be low, employers still need to create the right environment to avoid litigation.

Monitoring employees in a way that does not subject them to levels of surveillance that are demeaning and having clear rules that are applied consistently can go a long way in creating a trusting atmosphere and appropriate expectations for the privacy/security balance in the workplace.

Implementation

A preventive measure that will protect employers’ right to seek and obtain the information they need to protect their assets and provide a safe workplace while respecting employee privacy is to create policies and give notice to employees in advance. Some policies that address the employer’s right to monitor or conduct searches should include:

- Electronic communications:
- Telephones.

- Voice mail.
- E-mail.
- Internet and computer use.
- Company property and premises:
 - Company property including lockers, offices, desks and filing cabinets.
 - Personal property while on company or client/customers' premises.
- Safety and security:
 - Use of video cameras.
 - Electronic monitoring.

Tell employees (for example, during a new-hire orientation) of the employer's right to conduct searches, explain under what circumstances these searches may be conducted (generally at any time for any reason, with or without notice) and reinforce that no employee should have any expectation of privacy in his or her office, desk, filing cabinet, computer, electronic communications, lockers or even personal property while on company or client premises, including the employee's car. Require employees to provide copies of keys or disclose passwords, combinations or any other "security" measures to any member of management upon request.

In a world that faces ever-increasing threats and challenges--from domestic violence to acts of random or intended violence and crime--employers are obligated by law to provide a safe workplace. Communicating to employees in advance of the measures the employer has in place to protect them and why these measures are used will go a long way to securing employees' trust and cooperation.

Endnotes

¹Kaneilos, M. (2004, July 27). Under-the-skin ID chips move toward U.S. hospitals. *CNET News.com*. (See also: "First reported implanting of RFID chips in employees," www.hrprivacy.com/privacynews.html.)

²Institute of Management & Administration. (2004, May 1). Should payroll be looking into high-tech time clocks? *Payroll Mangers' Report*. (See also: Sasso, M. (2003, August 25). Some U.S. firms use video cameras, other technologies to watch workers. *Tampa Tribune*.)

³Teicher, S. A. (2003, December 22). It's 2 a.m. Do you know where your workers are? *Christian Science Monitor*. (See also: Baker, C. (2003, January 23). Channel 7 uses GPS to dispatch its crews; some workers see privacy invasion. *Washington Times*.)

⁴PR Newswire. (2003, September 8). *IBM ranks best, Eli Lilly work in employee privacy*.

⁵The Bureau of National Affairs. (n.d.). *HR practitioner's guide: Employee records*.

⁶Galkin, W. S. (n.d.). Electronic privacy rights: The workplace. *The Computer Law Report*.

⁷Social Security Administration. (2004, August 5). *House committee on ways and means approves H.R. 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2004*. Retrieved from www.ssa.gov/legislation/legis_bulletin_080504.html.

⁸BNA. (2004, April 8). Voluntary benefit protects workers from identity theft. *Bulletin to Management*.

⁹U.S. Federal Trade Commission. (n.d.). *Using consumer reports: What employers need to know*. Retrieved from www.ftc.gov/bcp/online/pubs/buspubs/credempl.pdf.

¹⁰<http://www.ftc.gov/os/statutes/2user.htm>

¹¹<http://www.ftc.gov/os/statutes/2summary.htm>

SHRM wishes to thank Christine Walkers, Mary Lee Lison, SPHR for contributing this paper. This paper is intended as information only and is not a substitute for legal or professional advice.

Christine Walters has nearly 20 years combined experience in management, human resource administration, employment law practice and teaching, and has received national and regional awards and accolades. She has presented at conferences across the country on a variety of employment and HR-related topics and has been interviewed in a variety of media, including the Wall Street Journal. Today she works as an independent consultant providing proactive human resource and employment law consulting services and is an adjunct faculty member of the Johns Hopkins University teaching in graduate, undergraduate and certification-level programs. Ms. Walters is a member of SHRM's Employee Relations Special Expertise Panel.

Merry Lee Lison, SPHR, has 18 years of human resource generalist experience and is the Vice President of Human Resources for Employee Benefit Consultants, Inc. in Milwaukee, Wis. She is an active SHRM volunteer at the student, local, state, area and national levels and is currently a member of the Employee Relations Special Expertise Panel. Ms. Lison holds a BBA from the University of Wisconsin-Whitewater and a MBA from Marquette University.

 **Back**