

## PRIVACY

Privacy is a constitutional right. As we become more technologically able to “tap in” on people's lives and secrets, there has been growing concern and litigation over invasions of our privacy. There have been a number of laws protecting privacy of employees, employee records, and employee communications (see attached listing). Some of these laws carry heavy damages and even criminal penalties.

A recent Harris Opinion Survey found that 79% of Americans are “seriously concerned” about threats to their privacy. Furthermore, 75% believe that their employers abuse their privacy rights and misuse information about them.

Invasion of privacy claims in employment generally arise when managers go too far beyond job relatedness or gather job-related information in an unreasonable way. Some areas currently giving rise to privacy cases are: drug testing, physical searches, locker searches, personal parcel searches (lunch box, purse, backpack), employer surveillance, e-mail and telephone monitoring, and breach of confidentiality.

Privacy cases generally involve one of three sorts of issues:

1. Looking into non-job-related private life;
2. Delving too deeply into expectations of privacy; and
3. Making private facts public.

### Looking Into Non-Job-Related Private Life

For too many years, employers made decisions based on factors such as:

1. Whether the employee went to church (and was it the “right” church?)
2. Was the employee married to the person they lived with?
3. Did the employee date or marry in the “right” ethnic or racial group?
4. Did the employee belong to “problem” social or political organizations?
5. Did the employee have a “proper lifestyle”?

None of these are directly related to the ability to honestly and capably perform a job.

Another form of this invasion occurs when off-work surveillance of job-related issues like sick leave, absence, or moonlighting cross the border into non-job related private life. When the monitoring goes on too long, looks into home windows, or involves questioning neighbors about the employee's comings and goings and habits, it often incorporates non-job privacy issues into the investigation.

### **Expectation of Privacy**

The major focus of this privacy area is an “expectation” of not having other people intrude, observe or listen without consent. There are a number of things on the work site which are also expected to be private. An employer that video monitors rest rooms to “catch drug deals” also videotapes the highly private act of people in the facility for its intended use. Audio monitoring a break area or telephone picks up personal conversations about romances, family problems, health and other confidences the speaker was only willing to share with the listener. Employees expect that the contents of their purses, lunch boxes, wallets or vehicles are private. Employees have a belief that their e-mail or voice-mail are private. Searches of desks and lockers have been the subject of privacy cases.

When one delves into these areas, it should be expected that people will feel “invaded” and be upset. Therefore, investigations or surveillance of these “expectations of privacy” areas should be done carefully with forethought and consideration of whether the need is great enough to balance out the invasiveness.

The main issue is the “expectation.” If people do not have an “expectation” that their conduct or communication is private then there is no “invasion.” Notice can be a major factor in the difference between invasion of privacy and the employers’ valid right to inspect or monitor. Advance, clear, written notice of the specific areas for monitoring or inspection lets people know not to expect their actions, communications or personal property to be private.

Be aware that notice does not give a *carte blanche* to go snooping into employees non-job-related personal lives. Even with notice, the more intrusive the search, the more “personal” the monitoring, the more the employer will be required to show a compelling job-related reason to justify the intrusion. So even if you give notice, you still can't go through people's purses and parcels without a powerful reason. Notice, also, does not take you out of the scope of laws, such as wire tapping which prohibit many forms of monitoring phone and electronic conversations.

### **Making Private Facts Public**

Employers have a lot of legitimately collected, directly job-related information which may still be embarrassing or harmful if it is not handled confidentially. You may have details in the files about employees' health, disabilities, family situations, disciplinary action, references, basis for hiring or promotional decisions or emotional conditions. Laws, such as the Americans With

Disabilities Act, require keeping some of this information in a separate and tightly controlled confidential file. Other sensitive information is not regulated by a law, but it can still result in privacy or defamation suits if it leaks. In one Wisconsin case, an employee was validly fired for wrongdoing, but then won a privacy case because the employer “advertised” the reason for the discharge to the rest of the work force.

In general, an employee's discipline, evaluations, health and other sensitive information are between them and their direct management only. The best practice is that only those in the direct chain of supervision who have a “need to know” and who are directly involved in decision making are allowed access to information about an employee.

The confidential information often leaks out when employment issues are discussed in non-confidential areas such as office cubicles without floor to ceiling walls or with thin walls, or in a cafeteria or break area where others can overhear. Home conversations about sensitive work issues often leak out on your children's school playground the next day and are carried home to other children's parents in the community. Leaving files lying around where others can see them leaks information. Having too many people involved in the process gives more opportunities for confidences to be spilled.

Interpreters who are not employees but come in to assist when language or disability require, often “leak” information because no one told them about the importance of confidentiality. All such interpreters or consultants should sign a confidentiality statement.

Organizations have the right to use sensitive job-related information to help promote effectiveness or prevent problems. However, once the direct purpose has been accomplished, it does not serve any valid purpose to spread that information to other employees who were not directly involved in the process. That spreading of confidential or sensitive information to others creates potential liability for invasion of privacy.

## QUALIFIED PRIVILEGE

Employers have to gather, keep and discuss information about employees in order to effectively manage. Some of this information is "personal and sensitive." Some is negative, such as poor performance evaluations, discipline or discharge. The employee at question does not want it "spread around," harming his career and reputation.

The Qualified Privilege or "conditional privilege" as it is termed in the chief Wisconsin case, *Bett v. Ploetz*, 20 Wis.2d 55 (1963), enables managers to gather and discuss this sensitive information without liability as long as one stays within the scope of the privilege.

The requirements one has to show to establish Qualified Privilege are:

1. The information is reasonably necessary for the protection of the interests of one of the parties. This criteria is automatically met by a current issue effecting someone in the scope of the organization's activities (job related). The organization has a great "interest" in finding out about and solving work-related performance problems, disability accommodations, or rule violations by its employees.
2. The scope of the inquiry is limited to what is reasonably necessary to protect the interest. This means job relatedness. Once the topic goes into family, religion, sexuality, politics, or other non-directly related areas, it has left the scope and protection of the defense, and the Qualified Privilege disappears.
3. The information is communicated on a proper occasion. This means it is a current issue within the time frames recognized by state and federal law or by internal procedures. Old "stale" issues are not within the Qualified Privilege. Similarly, where an employer is on a fishing expedition to dig up dirt on employees for office politics or gossip, there is no Qualified Privilege.
4. The information is given to and confined to proper parties only. "Proper parties" means the small group that must process that particular issue. It can include the Personnel Manager, Affirmative Action Officer and top management who have a direct role in the decision making.
5. The process is conducted in a proper manner.
6. The entire process is characterized by good faith.

## PRIVACY LAWS LIST

Privacy rights in employment are protected by a number of state and federal laws.

### STATE LAWS

Wis. Stat. §895.50: "Invasion of privacy" includes the intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a matter which is actionable for trespass and/or publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person.

Wis. Stat. §103.15: HIV Testing, confidentiality of results.

Wis. Stat. §146.82: Patient Health Care, confidentiality.

Wis. Stat. §51.30: Mental Health, Drug & Alcohol Treatment, and 42 U.S. Code §290, Drug & Alcohol Confidentiality, provides for confidentiality of treatment records. These laws prohibit unauthorized release and dissemination of medical and treatment information, including post drug and alcohol testing counseling.

However, Wis. Stat. §102.13(2) and §103.10 Family Medical Leave Act, as well as the Americans With Disabilities Act, do give the employer a right to access and use of certain medical or treatment information when an employee reports a work-related condition; but all medical information must be kept in a separate, secured file. The 1996 Federal Health Care Reform Act, H.R. 3103, imposes civil and criminal penalties on employers (and their agents) who disclose personally identifiable health information without consent.

### FEDERAL LAWS

18 U.S. Code §2501 et seq. Omnibus Crime Control Act/Electronic Communications Privacy Act (§2701 et seq.) prohibits the unauthorized interception and disclosure of wire, electronics or oral communications through the use of electronic, mechanical, or other devices. The Federal Act gives both civil and criminal penalties for violations. The Act does give employers the right to access email and voice mail in the employer's system (not a system provided by an outside company.)

42 U.S.C. 263, Health Insurance Portability Accountability Act, Patient Health Care, and Health Insurance Privacy and Confidentiality. HIPPA protects the privacy of medical information. Requires an information management process to assume privacy and prevent improper use. The law provides for civil penalties of \$25,000 per year, per violation and criminal liability.

20 U.S. Code §1232, Family Educational Privacy Act. Confidentiality of records of participants in educational programs receiving government funds (can include job training programs conducted in the work place).

18 U.S. Code §1702, Obstruction of Correspondence, Mail Privacy. It is illegal to read another's mail before it is delivered to the addressee. An employer can be liable for intentionally opening and reading employee's personal outgoing mail.

42 U.S. Code §290, Drug and Alcohol Confidentiality, provides for confidentiality of treatment records. These laws prohibit unauthorized release and dissemination of medical and treatment information, including post drug and alcohol testing counseling.

However, 29 U.S. Code §2601 et. seq., the Federal Family Medical Leave Act, as well as the Americans With Disabilities Act, 42 U.S. Code §12101, do give the employer a right to access and use of certain medical or treatment information when an employee reports a work-related condition, but all medical information must be kept in a separate, secured file.

15 U.S. Code §1681, Fair Credit Reporting Act, requires "accuracy, relevancy and proper utilization of information." This act covers not only standard "credit checks" it also covers employment references and investigations and examinations where outside parties are used as gatherers of the information.

29 U.S. Code §§2001-2009, Polygraph Protection Act, prohibits most private sector employers from requiring mechanical or electronic lie detector tests except under specific circumstances and from using the tests as the sole basis of making employment decisions. The Act also prohibits disclosure of the results beyond those directly involved in the investigation and decision making. This law does not prohibit written "honesty tests" (though some states do) [but also be aware that the ADA may apply if the "honesty test" is found to be "psychological testing"].

5 U.S. Code §522(a), Federal Privacy Act, prohibits federal agencies from disclosing personnel records without the employee's written consent. This can include improper disclosure to staff within the agency itself.