FAIR MEASURES, INC.

P.O. Box 2146 Santa Cruz, CA 95063
831-458-0500, fax 458-0181
www.FairMeasures.com
training@FairMeasures.com

Managing Within the Law II

reference materials

We gratefully acknowledge the contributions to these materials of all of the attorneys who have worked with Fair Measures: Rita Risser, J. Logan, Jonathan Levy, Ann Kiernan, Steve Duggan, Lynne Eisaguirre, Julie Crane, Joelle Sullivan and Michele Huff. We also are grateful to our clients, and their legal counsel, Human Resource professionals and Training Department staff, who have given freely of their ideas to improve this course.

None of Your Business?
The Law of Privacy and Drug Testing

What is Privacy?

Plaintiffs' lawyers, the attorneys who represent employees, predict that privacy will surpass wrongful termination as the hot issue of the new millennium. Yet the concept of privacy is so broad, it's difficult even to define.

Originally, privacy was defined as the "right to be left alone." This meant you could not intrude upon my seclusion or publicize private facts about me.

Today, the definition has expanded. Privacy includes ideas like human dignity or self-respect, and autonomy or self-governance. Privacy also has been called secrecy, anonymity, solitude, psychological integrity and personality. Privacy means you can't make me do what I don't want to do. What I do in private is none of your business. I have the right to control my own life.

Texas is one of the leading privacy states. One court there said, "The heart of this privacy interest is the individual's exclusive prerogative to determine when, under what conditions, and to what extent he will consent to divulge his private affairs to others."

The idea that one person could sue another for invasion of privacy is only 100 years old. Originally, only the government could be sued for invasion of privacy, under the Bill of Rights of the U.S. Constitution.

The First Amendment to the Constitution allows freedom of speech, religion and of assembly. Freedom of assembly also is referred to as freedom of association, and means that people are allowed to gather and join with others as they wish.

The Fourth Amendment prohibits unreasonable searches and seizures of "persons, houses, papers and effects." It protects our most personal spaces.

The Fifth Amendment provides that no one can be compelled in a criminal case to be a witness against himself. Also known as the privilege against self-incrimination, this amendment protects our minds from intrusion.

These Amendments, by their terms, only limit the power of the government. For the most part, they have been applied to put limits on the police. But they also have been interpreted to protect employees who work for the government.

For example, a woman worked for a county sheriff in Texas in 1981. When she heard that President Reagan had been shot but not killed, she said, "If they go for him again I hope they get him." She was fired on the spot.

The U. S. Supreme Court held she could not be fired. She worked for a governmental agency. She was exercising her freedom of speech. She could not be deprived by the government-employer of her freedom to speak out on a matter of public interest.

What of the rights of employees who work for non-government employers? Historically, they didn't have any privacy. In the 1920's and 30's, Ford Motor Company checked the cleanliness of employees' homes, the neatness of their gardens, their attendance at church and the kinds of cars they drove. Employees who didn't meet the company's standards legally could be fired.

Ford employees couldn't sue for invasion of privacy because the Bill of Rights didn't apply to them.

It didn't seem fair that government employees had freedom of speech and other privacy protections when non-government employees didn't. But if the Bill of Rights didn't apply to them, what law did?

In 1890, the idea was proposed that everyone has a common law right to privacy. In 1905, the Georgia Supreme Court was the first to say that people have the right to be free of intrusion upon seclusion.

Today, the right of privacy is recognized to some extent in every state. This right protects us from invasion of privacy by the public, the press and employers.

In this chapter, we will be giving examples from many different states. Most of these cases would be decided the same in any state. These cases illustrate generally accepted privacy principles.

Craig Cornish, an employee's attorney from Colorado who is recognized as a national expert on workplace privacy, says there are six types of privacy cases. The six types, and the issues they raise can be seen in the box.

type of privacy issue	situations where it occurs
collecting information	drug tests
method and means of collection	polygraphs, searches, mail, telephone & computer monitoring, video surveillance, shadowing
retaliating against employees who refuse to give information	questioning employees, wrongful termination
using private information against the employee	free speech, sexual orientation protection, arrest records, defamation, false light, appropriation
disclosing private information to others	revealing medical information, personnel files, home address & phone
infringing the dignity of the employee	asking personal questions, relationship restrictions, lifestyle discrimination, appearance standards, use of tobacco, alcohol or other legal substances; engaging in any lawful activity outside of work

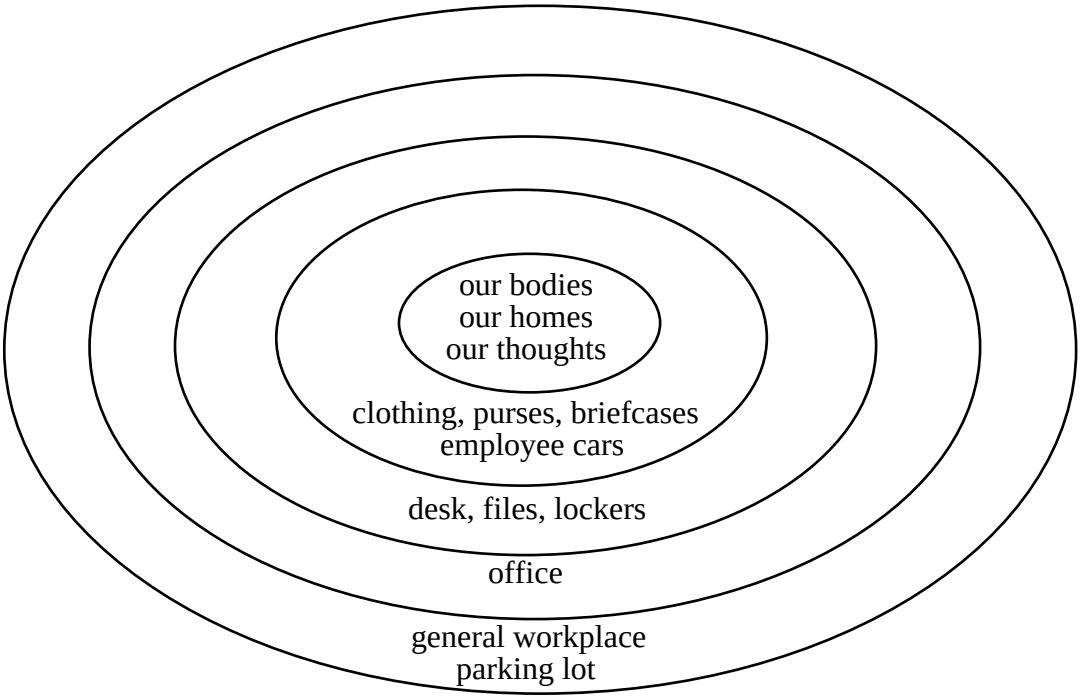
All of these situations will be discussed in this section.

To analyze whether any of these actions is an illegal invasion of privacy, courts use different legal standards. A simplified version of the analysis courts use in privacy cases is this four-step process:

--what is the zone of privacy being invaded?
--what is the person's reasonable expectation of privacy?
--is there a sufficient reason to justify intrusion?
--are the means used rationally related to the end sought?

Zones of Privacy

The zones of privacy can be seen in the illustration below. The areas in the center are the most personal: our bodies, our minds and our homes. Next most personal is our personal belongings. Less personal is the desk and files we have at work. Less still is the office we use, then the general workplace, and last the parking lot.



Reasonable Expectation of Privacy

Once you know what zone of privacy is affected, you can determine the reasonable expectation of privacy. The zones closest to the center have the highest expectation. For example, we have a very high expectation of privacy in the contents of our pockets. We don't expect other people to go through our pockets without our permission. The more personal the zone of privacy, the higher the expectation of privacy.

An employer can change employees' reasonable expectation of privacy in some cases by notifying them in advance that the company reserves the right to invade their privacy. The employer's right to do this, and limitations on this right, will be discussed if applicable in each section below.

Reason to Invade Privacy

Even if we have a reasonable expectation of privacy, the law still may allow our privacy to be invaded if there is sufficient reason to justify it. A "compelling interest" is required to invade areas that have a high expectation of privacy. A "rational basis" is required to invade areas with lower expectations of privacy. Both of these are higher standards than the "business necessity" standard discussed in the chapter on discrimination law.

Just as police officers must have reasonable suspicion before they can search people, employers must have compelling or rational reasons to invade privacy:

reasonable suspicion of theft at work
reasonable suspicion of intoxication at work
maintaining plant security
measuring work performance
protecting trade secrets
ensuring workplace safety
preventing bribery of employees
preventing conflicts of interest

Means Reasonably Related to Ends

Assuming the employer has a compelling or rational reason to invade privacy, then the means chosen must be rationally related to the end sought. This is determined through a balancing test. The need of the employer to obtain information is weighed against the extent to which the employee's seclusion is invaded.

For example, if a company wanted to protect trade secrets, it might decide to prohibit employees from dating employees who work for competitors. But if such a policy applied to all employees, whether or not they had access to trade secrets, it would not be rationally related to the ends sought. We would say the policy is overbroad. It would be interfering in the private lives of many employees, when only a few employees are at risk. Therefore, such a broad policy is an invasion of privacy.

When there are alternative means that don't invade employees' privacy but achieve the same result, the balance is likely to tilt in favor of the employee. For example, if the no-dating policy above applied only to people with access to trade secrets, it still invades their privacy, but the

policy is reasonably related to the ends sought and is more likely to be upheld.

The problem of overbroad policies can best be seen in the controversy surrounding drug testing.

Drug Testing

There are six types of drug tests: pre-employment to screen out applicants, "for cause" testing of employees upon reasonable suspicion of intoxication, post-accident, regularly scheduled tests (usually part of a general physical), unannounced random tests, and follow-up tests to confirm an employee is maintaining sobriety after testing positive.

The Department of Defense (DOD) requires non-commercial defense contractors to drug test some employees. Covered companies also are required to have drug awareness education, employee assistance and rehabilitation programs, and procedures for identifying illegal workplace drug use.

Under DOD rules, employees must be drug tested if they have access to classified information or are in positions that, for reasons of national security or health and safety, require a high degree of trust and confidence. It is up to the employer to decide what type of testing to perform. However, if state or local laws or union contracts prohibit drug testing, DOD contractors are not required to test.

The U.S. Department of Transportation requires drug testing for drivers in interstate commerce, airline personnel and railroad employees. These regulations require pre-employment, for cause, post-accident and random tests for sensitive positions.

Even if a transportation worker tests positive, rehabilitation may help the worker keep his job, as the U.S. Supreme Court decided in 2000. In that case, a man who worked on a road crew and drove heavy vehicles on public highways tested positive for marijuana and was fired. His union went to arbitration, and he was reinstated on the condition that he go in to substance abuse therapy and agree to random drug tests for five years.

Fifteen months later, the worker again tested positive for marijuana, was fired, and was reinstated by the arbitrator with the same conditions, plus requiring him to pay for the arbitration and to give his employer an undated letter of resignation, which would immediately take effect if he

tested positive a third time. The company sued to overturn the arbitrator, arguing that the second reinstatement was against public policy.

The Supreme Court unanimously acknowledged the company's argument that a purpose of the DOT law and regulations was to rid the roads of impaired drivers, but also pointed out that rehabilitation was another important purpose. After stressing that his job depended on the worker's compliance with rehabilitation, the Court ordered that the worker be reinstated.

According to a 2008 study by the American Management Association, 55% of employers do new-hire drug testing, and 44% do employee drug tests. According to one of the country's largest drug-testing laboratories, in 2006 less than 4% of the workers who were tested randomly came up positive. Even when an employer had a reasonable suspicion of intoxication, more than 80% of the tests came back negative.

But just because all of this testing is going on, doesn't mean it is legal. Many drug tests have been challenged, and in many cases the employees won, because the tests illegally invaded their privacy.

Let's go back to the four-step process for analyzing privacy claims to see how the courts have decided the drug testing cases.

1. What is the zone of privacy? Drug tests invade the most personal zone -- our bodies, our minds and, by extension, our homes. From analyzing urine, much more can be known about our private lives than illegal drug use. In order to have accurate test results, employees must disclose the prescription and over-the-counter medications they take. Thus an employer will know about medication taken for diabetes, epilepsy, high blood pressure, HIV, depression, birth control and many other sensitive medical conditions.

2. What is the reasonable expectation of privacy? Drug tests normally are based on urine samples. As the Supreme Court has noted, passing urine is one of the most private things we do in our society. It is done behind closed doors. It's illegal if done in public. And in drug tests, not only must we pass it on demand, but often someone watches as we do it.

As a New Jersey court put it, "We would be appalled at the spectre of the police spying on employees during their free time and then reporting their activities to their employers. Drug testing is a form of surveillance, albeit a technological one. Nonetheless, it reports on a person's off-duty activities just as surely as someone had been present and watching. It is George Orwell's 'Big Brother' Society come to life."

3. Is there sufficient reason to invade privacy? The U.S. Supreme Court has held that employers must have a compelling reason to drug test, and has found drug testing justified in two instances.

The Court has said railroads have a compelling reason to test employees for drugs immediately after train accidents. The Court reasoned that the fear of having a drug test would discourage employees from taking drugs. A decrease in drug use presumably would decrease accidents and increase passengers' safety. Society's interest in protecting the safety of passengers outweighs the railroad crews' right of privacy.

In another case, the Supreme Court said there was a compelling reason to give drug tests to candidates for promotion in the U. S. Customs Service. Customs officers' jobs require them to search for illegal drugs. Drugs often are in their possession and control. If the government hired drug abusers in those jobs, they could be susceptible to bribery and might have a conflict of interest between their addictions and their jobs.

4. Are the means rationally related to the end sought? This is where the problem of an overbroad test comes in. In the first year of post-accident testing, 3.8% of all railway accidents involved employees who tested positive for drugs. In 1991, only 2.6% tested positive. So 97% of the good, honest employees who were involved in accidents suffered the added insult to injury of being treated under suspicion, guilty until proven innocent.

Similarly, the Customs officer case relies on faulty assumptions. In his dissenting opinion, conservative Supreme Court Justice Scalia pointed out that just because employees use drugs doesn't mean they are likely to accept bribes from drug dealers, any more than officers who wear diamonds are likely to be bribed by a diamond smuggler.

"Nor is it apparent to me that Customs officers who use drugs will be appreciably less sympathetic to their drug-interdiction mission, any more than police officers who exceed the speed limit in their private cars are appreciably less sympathetic to their mission of enforcing the traffic laws."

Another reason drug tests are overbroad is they do not measure current impairment. Unlike blood alcohol tests, which detect the amount of alcohol currently in one's system, drug tests generally only measure inert metabolites that are the end products of drugs. These metabolites have no psychoactive effect themselves, and they are excreted from the body

more slowly than drugs. Drug tests show past drug use; they do not show current impairment.

The U.S. Supreme Court has recognized the problem of overbreadth, and generally has required proof of impairment at work. In a 1987 case, the Court allowed a papermill worker, Mr. Cooper, to be reinstated to his job. He was fired after he was found in the company parking lot in his car, which was filled with marijuana smoke. Gleanings of marijuana later were found in the upholstery.

The Supreme Court said, "The assumed connection between the marijuana gleanings found in Cooper's car and Cooper's actual use of drugs in the workplace is tenuous at best."

Drug tests are overbroad for another reason: many studies have found alarming rates of false positives. The most optimistic study found that 1% to 2% of the samples tested positive for drugs when in fact no drugs were present. Although proportionately small, given that 10 million employees are tested each year, hundreds of thousands are being falsely accused of drug use on the basis of faulty tests. Some experts believe the rate of false positives is as high as 62%.

Finally, there are less intrusive alternatives to drug testing. Performance Factors, a California company, has developed tests that measure people's reaction time, visual acuity and other job-related abilities. Much like a video game, the test is used by employers such as railroads, steel mills and transportation to test employees at the beginning of each work day.

This test does not invade privacy. Unlike drug tests, it catches people when they're impaired, before they get into accidents. And it catches them when they can't perform for reasons other than drugs, such as lack of sleep, depression or hangovers.

Despite the problem of overbreadth, the Supreme Court upheld drug testing of railroad employees after accidents, and of Customs officers. Other federal courts have upheld testing for other jobs. See the box on next page for the drug tests that have been upheld.

Random Drug Tests Allowed

In these cases, the courts have allowed random and all other drug tests for employees in sensitive positions:

employees with national security clearances
airline personnel
corrections officers with prisoner contact
transportation employees
employees at chemical weapons plants
Army civilian employees
employees with top secret clearances
police officers
nuclear power plant workers
water treatment plant workers

Some federal testing requirements have not been upheld. The U. S. Department of Agriculture was sued for requiring all Food and Nutrition Service employees to be tested if the supervisor had reasonable suspicion of off-duty drug use.

The agency argued it had a legitimate interest in stopping off-duty use: users' work performance might be affected, they might buy drugs at work or steal to support their habits, and their drug use might erode public confidence in the agency.

The Court of Appeals said this was mere speculation and could not justify invasion of privacy. The court held that testing for off-duty use might be upheld for workers in safety- or security-sensitive jobs. But other workers could not be tested unless there was reasonable suspicion of on-duty drug use or drug-impaired work performance.

Further, a 1998 national study of the computer and communications equipment industries cast serious doubt on the assumption that drug testing improves productivity. The Le Moyne College Institute of Industrial Relations study results suggest that drug testing has served to lower rather than enhance productivity. Why? First, drug tests can be expensive, considering the costs of implementing a drug test program, and conducting the testing, including not only the price of each test but also the time taken by employees to either administer or take the tests. If there is a positive test result, then there is the cost of a second test because of the possibility of a false-positive. Second, the study authors suggest that

drug testing could undermine worker morale and loyalty, because a sizeable number of employees believe drug tests, particularly random tests, are unfair. Those workers may not be as motivated to contribute, may seek employment elsewhere, and may choose not to accept jobs from companies with drug testing programs.

State Drug Testing Laws

These federal court decisions are only the beginning. There is much more to the law of drug testing. Every state has some privacy protections, and 15 states have statutes specifically regulating drug tests.

A state's privacy statute may be interpreted by that state's courts more broadly than the Supreme Court interprets the U. S. Constitution. If the state's law gives more protection to privacy, generally it must be followed instead.

In California and many other states, pre-employment testing has been upheld, but not random tests for employees in non-sensitive positions. Even when they hold safety-sensitive positions, California employees have a right to privacy off-duty. A CalTrans equipment operator was fired when he failed a drug test, but CalTrans reduced the punishment to suspension after the worker agreed to random follow-up drug testing. When one of those tests, done during time off, showed drug use, the worker was fired. In a 2000 decision, a California appellate court reinstated the worker—with back pay—holding that his constitutional right to privacy during time off had been violated. And in 2004, Arizona's Supreme Court ruled that random, suspicionless testing of firefighters violated their state and federal constitutional privacy rights.

Most state courts that have ruled on tests allowed pre-employment and post-accident tests. Reasonable suspicion of on-duty drug use also has justified tests, as long as the manager was able to document why he or she had reason to believe the employee was on drugs. Reasonable suspicion is very difficult to prove. According to Quest Diagnostics, a major drug testing laboratory, about 85% of the people sent for testing based on reasonable suspicion tested clean. Each one of those people may have a claim for invasion of privacy.

A 1997 California appellate case is an example of the disasters that await employers who attempt reasonable suspicion testing. One day, a senior manager saw an executive secretary sitting with her elbows on her knees, looking down at the ground. When she did not move, he asked her what was wrong and she didn't answer. He then called the HR director

and told her that he thought the secretary might be having "female problems."

The HR director observed that the secretary's "speech was slurred, that her demeanor was lethargic, that she was swaying, that her eye contact was not there, that it seemed to be deliberate in the answers, it was very controlled and very deliberate." Based on these observations, the secretary was ordered to take a drug test, and when she refused, she was fired.

Both the senior manager and the HR director admitted they had never received formal training on detecting substance abuse. The court also found it significant that the secretary was told to drive herself to the lab for drug testing! What's more, after she was fired, she was allowed to drive herself 60 miles home. To the court, these facts implied management did not believe at the time that she was truly impaired, and the secretary was allowed to continue her suit against the company for invasion of privacy and wrongful termination.

State drug test statutes also vary widely. Some states, such as Utah, almost encourage employers to drug test. Other states limit employers' use of tests.

For example, Maine's law requires employers with 20 or more full-time employees to have an employee assistance program before beginning any drug testing. Employers' drug prevention and testing policies must be approved by the state before being implemented.

The Maine statute also regulates how test samples are collected. Employers are allowed to drug test all applicants, and employees may be tested if they are suspected of using drugs at work. Random tests are allowed only in safety-sensitive positions, or for employees who are undergoing rehabilitation.

In Maine, you can't terminate employees for drug abuse unless you first give them the opportunity to participate in a rehabilitation program for at least six months. If employees refuse rehabilitation, they can be terminated immediately.

Whether or not your state has a drug law, drug tests may not be given in a discriminatory manner. If applicants are to be tested, all applicants for the same jobs must be tested.

If drug tests uncover employees addicted to drugs, you may be required to offer them rehabilitation under your state's law, or under a union agreement.

> ***practical pointers:*** Because this is a volatile area, it is highly recommended that you conduct a full investigation of the law and practice in your community and industry before you begin a program. Consult with attorneys and other experts to implement drug testing. See the box for a checklist of items to consider before starting drug testing.

Drug Testing Checklist

identify a reputable testing lab
prepare legal notices for employees/applicants to read and sign
establish the mechanics of obtaining samples, including whether people will be monitored while giving the sample
establish chain of custody controls so samples are not confused or tampered with
budget to include a second (different) test in case of positive results, to minimize possibility of false positives
designate an individual in your company to receive test results
establish confidentiality controls for test results
decide how employees/applicants will be informed of results
provide process for appealing the results
establish procedure for referring them to rehabilitation

If you don't have a testing program, what should you do about drugs in your workplace? If you suspect employees are abusing drugs or alcohol, document the objective, verifiable facts that prove their work is affected. You want to show they are arriving late, falling asleep or slurring their words. Document their emotional mood swings and irrational outbursts. Start a program of counseling and disciplining them just as you would anyone else who isn't performing.

Even if you have a drug testing program, you still must document poor work performance to justify your reasonable suspicion for ordering an employee to take a test.

Don't do what one manager did. He fired an employee for documented poor performance. But when he fired him, the manager said, "Off the record, I think you're a drug addict." There's no such thing as off the record. Such an accusation could lead to a claim of

defamation, intentional infliction of emotional distress, or invasion of privacy.

Federal Drug-Free Workplace Act

One other statute applies to drugs. The U. S. Drug-Free Workplace Act requires all federal government agencies and contractors, including vendors with purchase orders totaling $25,000 or more, to adopt a policy statement and distribute it to employees.

It also requires companies to develop drug awareness programs. The program must include information on the dangers of workplace drug abuse, the company's anti-drug policy, and the penalties for violating the policy. You also must inform employees of any available rehabilitation and counseling programs. Some states have adopted similar programs for state government contractors.

The right to privacy involves much more than drug tests. In the following sections, we'll cover the other protected areas.

Polygraph (Lie Detector) Tests

Lie detector tests aren't considered reliable. For that reason, they are illegal in almost every situation under U. S. law. The U.S. Supreme Court says they are not admissible evidence in court. The Employee Polygraph Protection Act of 1988 prohibits employers from requiring, requesting or suggesting that employees or applicants take lie detector tests. Employees can't be fired, disciplined or discriminated against for refusing to take them.

If you violate this law, you can be fined up to $10,000 by the Department of Labor and sued by the employee.

There are a few exceptions. This law, like many other federal laws, does not apply to the U.S., state or local governments. Contractors of the Department of Defense, National Security Agency and the FBI may be required to take polygraphs under certain circumstances.

Some private security companies can give polygraphs if their employees are hired to protect facilities that have a significant impact on the health and safety of citizens, such as nuclear power plants, toxic waste dumps and banks.

Any employer can ask an employee to *voluntarily* take a lie detector test *if:*

--it is part of an ongoing investigation into theft, embezzlement or industrial espionage, *and*
--you have a reasonable suspicion that the particular employee was involved, *and*
--you inform the employee of the right to refuse to take the test.

If employees refuse to take polygraphs, you cannot use their refusal to "prove" their guilt.

If a test is given, there are numerous requirements about what employees must be told, what questions can't be asked and how the information obtained can be used. A competent polygraph examiner will be aware of the legal requirements.

These exceptions don't apply if your state's law is more favorable to employees. For example, in California all polygraph tests are forbidden except for employees of state and local governments. In New Jersey, only employees of pharmaceutical manufacturers can be tested.

> ***practical pointers***: How do you discover the truth if you can't give polygraph tests? Hire an expert investigator. Many private investigators are expert at judging when people are lying. They also can bring more objectivity to your investigation.

Searches

If the police conduct an illegal search, the "fruits" of the search can't be used later in court. By analogy, it would be illegal to fire an employee as a result of the fruits of an illegal search.

Searches of employees' purses, briefcases, pockets and cars without their consent can be justified only if you have a compelling reason, such as reasonable suspicion a particular employee is hiding stolen property or is in possession of drugs.

Another good reason is a harassment investigation. In a state supreme court case from 2001, an employee received an obscene phone call on her voice mail. She thought she recognized the voice as that of a co-worker, and reported it to the security officer and her supervisor. Both of them independently listed to the tape, and identified the same man as the speaker. The suspected co-worker was asked to submit to voice print analysis, refused, and was fired. The court dismissed his wrongful termination suit, finding that the employer's actions violated no public policy.

Mundane business reasons also may justify searches. For example, in one case the employer, a lawyer, was allowed to search another lawyer's briefcase in order to retrieve some documents due in court. In a 2007 Florida appellate case, a man had been suspended for fighting with a co-worker. As he was leaving the workplace, his boss asked to inspect his briefcase to make sure he was not taking home any company property. The employee refused, saying he had personal items mixed in with company property. He was fired for refusing to cooperate, and the court upheld the denial of unemployment benefits, finding that company policy clearly said that an employee's refusal to allow the search would be considered "direct insubordination."

> ***practical pointers:*** Inform employees of your intent to search and do so in their presence. If this is not possible, the search should be witnessed and documented so you can't later be accused of indiscriminately rummaging through their personal things. If possible, consult with legal counsel before conducting search.

Searches of Company Property

Companies assign employees lockers, cars, desks and filing cabinets so they can do their jobs. Searches of company-provided items are generally less of a threat to privacy. But the courts will treat company property like employees' personal property if that's how you treat it.

Company lockers are relatively private, because they usually are reserved for personal belongings. But where employees sign agreements or there is written company policy that lockers may be searched at any time, there is no violation of the right to privacy when the lockers are searched.

Where there is no written policy, how much privacy lockers are given depends upon who has keys.

If the company provides the locks and employees are issued keys or combinations, they don't have any real expectation of privacy. They know the company could go in and look at any time.

If the employee provides the lock, and doesn't give a key to the company, the employee has a higher expectation of privacy. In one Texas case, the court held it was an invasion of privacy for K-Mart to break open employees' locks to search every locker for items missing from the store.

A company-provided desk may be protected from invasion of privacy. According to the U. S. Supreme Court, whether employees have a reasonable expectation of privacy in their desks is decided on a case-by-case basis. Where there is a high expectation of privacy, searches must be reasonably related to a legitimate purpose, either work-related or an investigation of misconduct.

In some companies, it's not uncommon for co-workers or supervisors routinely to look in employees' desks for office supplies, missing files or other work-related items. If anybody could go in the office and open the drawers, there is a low expectation of privacy. If the company routinely searches offices for security reasons, the employee can't reasonably expect privacy.

But if the desk has a lock and the employee has the only key, the employee has a higher expectation of privacy. In an Illinois case, the fact that a manager had given his secretary the key to his credenza meant he lost his expectation of privacy.

A company car assigned to one person may be very personal, depending upon who else has a set of keys. A car used by many others is less personal. But the glove compartment and the trunk might have more privacy if they are locked.

File drawers would seem to be the least personal, unless they are locked and the employee has the only key. Files themselves are considered company property unless marked "personal."

Even where you have the right to search, it is not unlimited. Clothes hanging in a company locker, purses inside desks, and briefcases inside company cars have higher expectations of privacy. They should not be opened without a compelling reason.

> ***practical pointers:*** Most companies want to protect themselves from employees walking in with weapons or walking out with inventory. You can have policies that reserve your right to search company property and personal belongings. You can keep duplicate keys for desks and lockers. That way you don't create an unreasonable expectation of privacy among employees. At the same time, your policy can affirm your respect of employees' privacy where it is unrelated to work performance.

Mail at Work

The law allows an employer to open the mail addressed to the business or its employees, for any legitimate business reason. The postal regulations (Domestic Mail Manual, Sec. 508.1.1) require that all mail addressed to a governmental or nongovernmental organization or to an individual by name or title at the address of the organization is delivered to the organization, as is similarly addressed mail for former officials, employees, contractors, agents, etc. If disagreement arises where any such mail should be delivered, it must be delivered under the order of the organization's president or equivalent official.

In other words, once the Postal Service carrier delivers the mail to a business, it's up to the business to decide how to distribute it internally. But, an employer can't obstruct delivery of employee mail, or destroy it, or open it with the intent of prying. Those are all federal crimes! (18 U.S. Code Secs. 1701-1703)

The privacy of mail received at work depends on the appearance of the mail and the company's practice or policy.

Generally, there is a low expectation of privacy in mail received at work that appears to relate to work. When employees are away from work, usually it is expected others will read and perhaps respond to their business mail, and save personal notes for their return.

Even when the employee is at the office, if a clerk routinely opens and sorts business mail, there is no expectation of privacy.

But mail marked "personal" or "confidential" has a high expectation of privacy. It cannot be opened without a compelling reason. Not only is the privacy interest of your employee to be protected, but also the privacy of the sender.

What is the expectation of privacy in interoffice mail? It depends on how it is sent: face up, in an unsealed envelope, in a sealed envelope, or sealed and marked "personal."

In the fall of 2001, letters containing anthrax spores were mailed to several news organizations and two U.S. Senators, killing five people, infecting 17 others, and contaminating dozens of buildings. The cleanup took years and cost more than $200 million. As a result of that bioterrorism incident, many organizations implemented policies that required all mail and parcels to opened in a central location. A well-written policy would

give employees the clear understanding that even mail marked "personal" or "confidential" would be opened as part of the organization's security procedures.

While the mail remains generally safe, the United States Postal Service has issued recommendations on how to reduce the risk of exposure to anthrax and other biological contamination. Visit www.usps.com for more information. If you receive an anthrax threat, call 911!

Computer Files & E-mail

At high tech companies, policies state they reserve the right to search computer files. Yet all employees have their own private passwords (keys) and many programmers encrypt their files to prevent reading by others.

Electronic mail (e-mail) is correspondence among employees, just like interoffice mail. E-mail also can be sent between employees and outsiders, like U.S. mail. To a programmer, most e-mail is open for the world (and the employer) to see. But many non-programmers mistakenly believe passwords keep their e-mail confidential. A Texas appeals court ruled in 1999 that when an employee stored e-mail messages under a private password on his workstation he did not have a legitimate expectation of privacy in the contents of the files. The court explained that the company's interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system outweighed any claimed privacy interest.

These companies also have policies prohibiting employees from reading each other's computer files and mail. Whether courts will say these policies create an expectation of privacy remains to be seen.

Absent a policy, should the company have the right to read e-mail or computer files? The Electronic Communication and Privacy Act specifically provides that e-mail systems provided by the employer belong to the employer and may be accessed at any time for any business reason.

In 2001, a federal trial court ruled that an employee had no legitimate expectation of privacy in his stored e-mail, and that employers have the right to read all e-mail received or sent by employees on the company e-mail system—even if the employee is working from home. A 2007 federal appeals case held that a man who brought his own computer to work did not have a reasonable expectation of privacy.

But the employer's rights are limited. A federal appeals court held in 2002 that a company cannot monitor a secured, independent website set up by an employee. In that case, a pilot had set up such a website, which criticized the company's position on labor negotiations with the pilot's union. Employees—but not managers--could access the site only if authorized by a username and password. An airline vice president obtained a username from an employee and viewed the website. The court held that the vice president's unauthorized viewing of the website did not violate wiretap laws, but might violate the Stored Communications Act. The court made it clear that viewing an employee's unsecured website would not be a problem. A Pennsylvania appeals court had reached the same conclusion in a 2000 opinion.

Company telephone answering machines and voice mailboxes are also treated as company property under the Stored Communications Act, and can be monitored and reviewed, if employees are advised of company policy in advance.

Even if mail is private, you can read it if you have a compelling interest. For example, a company received a sexual harassment complaint from a woman who was sent pornographic e-mail by a man at work. Disgusted, she erased it. After several weeks, she decided to report him. The company had the right to search his computer files for that day to see if he had saved a copy of the offending message.

> ***practical pointers:*** While searching files, whether on paper or computer, do not look in files clearly unrelated to the purpose of your search. Once you open a file, if it is not what you are looking for, immediately close it. Save items marked "personal" for last. Don't reveal personal information you learn to anyone else without a need to know.

Monitoring Telephone Calls

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 restricts when employers can listen to telephone calls, whether on an extension or through more sophisticated means. The law applies to anyone who uses the phone.

Phone monitoring generally is allowed in the ordinary course of business. For example, companies may monitor their customer service representatives, telemarketers and order takers.

When monitoring calls for business reasons, you can't continue to listen once you realize a call is personal. Personal calls only may be monitored

to determine if a call is personal or not. As one court put it, "a personal call may be intercepted in the ordinary course of business to determine its *nature* but never its *contents*."

Personal telephone calls can be listened to only if the employee is notified and consents to it. This consent can't be implied just because the employee has been notified the company has the capability or practice of monitoring. Consent is only implied if the employee knows the line is being monitored at a particular time.

For example, in an Oklahoma case, the employee knew the line was always monitored. He had been warned repeatedly not to make personal phone calls on this line, and other phones were provided for personal use. In that case, it was implied that he agreed to be monitored.

In twelve states, California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington, not only do you have to notify the employee, you also must notify the person on the other end. Both sides must give their consent. In Georgia, employers must obtain a license to monitor from the state Public Utilities Commission.

Monitoring Computer Usage

Computer-based monitoring is the computerized collection, analysis and reporting of information about employees' work activities.

Computer-generated statistics are used to evaluate part or all of the work performed by about 4 to 6 million office workers in the U.S. Employees such as data entry clerks, reservation agents and directory assistance operators have their key strokes counted by their machines. Many more millions of employees have computer statistics collected on them every time they use their terminals, but these records currently are not used to evaluate their performance.

Computer monitoring may soon be restricted, if any one of several bills proposed in Congress passes. One proposal regulates the collection, storage or analysis of information concerning an employee's activities by means of a computer, telephone call accounting or other forms of surveillance.

Also proposed is legislation that does not allow employers to collect information which is not relevant to the employee's work performance. It requires companies to give employees notice of the monitoring, allow

them access to the information collected and restrict disclosure of information to management or other employees with a need to know.

Whether or not this particular legislation is passed, this type of monitoring is controversial, and may be the subject of state laws. Computer monitoring also has led to claims for stress disability under workers compensation.

In a 2008 appellate case, a city gave text pagers to police officers. The city's policy on computers, Internet access and e-mail, which also applied to pagers although they were not specifically mentioned, stated this equipment must be used only for City business and that users have no expectation of privacy.

So far, the City was sloppy but probably safe. But despite the fact that the written policy said equipment must be used only for City business, officers routinely used pagers for personal messages, the City knew it, and even charged them for it! Talk about torpedoing your own policy!

One officer paid the overage fee month after month. His Lieutenant told him and other officers that as long as they paid for the extra messages, he would not audit them to determine which ones were personal. Thus the Lieutenant's oral policy, and the practice of accepting and processing monthly overage payments from this and other officers, contradicted the written policy. Then - surprise! - the Lieutenant secretly ordered transcripts of the texts and found - surprise! - sexually explicit material.

Was the police officer fired? Of course not. He sued for violation of his right to privacy and won, because the court held that he had reasonably relied on the Lieutenant's assurances that his messages would not be audited. Was the Lieutenant disciplined for establishing an informal policy in contradiction to the City's written policies and then violating his own policy by ordering the transcripts and causing this lawsuit? He certainly earned it!

> ***practical pointers:*** Make sure company policies cover all forms of technology, and that they are not being routinely violated by manager's practices. Policies should provide that no manager has the power to contradict them. And all managers need to be trained in your policies and their responsibilities in enforcing them, not making up their own.

Watching Employees

Watching employees at work is a time-honored method of supervision. There is no invasion of privacy in that, because the employee knows the supervisor is there.

Claims have been made where spotters, checkers or undercover investigators are brought in by the employer to watch employees. For example, employees who work for retail stores and bus companies routinely have their performance checked by auditors posing as shoppers or bus riders. Generally, this has been held not to be an invasion of privacy.

As an alternative to drug testing, companies have hired undercover investigators to identify employees who are using, buying or selling drugs on company property.

To date, the use of undercover investigators has not been found to be an invasion of privacy.

Another form of undercover surveillance is the use of video cameras. If video cameras also capture sound and are used to monitor telephone calls, they are subject to the same rules as telephones.

Using video cameras with or without sound also would be restricted by the proposed legislation that covers computer monitoring.

Even if there are no special statutes, common law privacy would allow you to video employees only for work-related reasons and only if they are informed of it. Videos cannot be used in places where there is a reasonable expectation of privacy, such as in the bathroom.

In the 21st century, you can't ignore picture-taking cell phones, either. In the workplace they pose a risk to employee privacy in restrooms, lactation rooms, the gym and locker rooms. They are also a potential security problem, and should be banned from areas where trade secrets, medical records, and other confidential information are stored.

Following Employees

Since one of the most protected zones of privacy is our homes, you might think employers could not follow employees to their homes or watch them once there. But for the most part, shadowing employees had been held not to be invasion of privacy.

In one case, the employer, a private security company in Louisiana, watched who went to and from the employee's home, took down the license plate numbers and ran license checks on each guest. This was held not to be an invasion of privacy because comings and goings are open for anyone in the public to see.

How far an employer may be able to go is illustrated in a Michigan case. An employer hired two private investigating firms after an employee filed a claim for workers compensation. The private investigators entered the employee's home under false pretenses to look around, watched him inside his home through the windows, and followed him to his doctor's office. They even flagged down the garbage truck and asked the driver about the employee's health.

This was held not to be invasion of privacy because, according to the court, the intrusions would not be objectionable to a reasonable person since the employer had a legitimate right to investigate the employee's claim that he was disabled.

In a 2007 federal appellate case, an employer suspected that a night-shift employee who claimed she was taking intermittent FMLA leave for migraines was really working for her husband's landscaping business during the days. They hired an off-duty police sergeant to conduct surveillance. One morning, after she had taken the night off for a claimed migraine, the officer followed her from her house to a local gas station, where she filled up two gas cans and drove to a cemetery that was one of her husband's customers,. She spent the day mowing at the cemetery before returning home and calling in to work that night with another alleged migraine. In upholding the employer's right to terminate her, the court noted that this was not interference with her FMLA rights, since the employer had "an honest suspicion" that she was abusing FMLA.

But even where the employer has the right to investigate, watch, trail, shadow or keep employees under surveillance, it can't be done in an offensive or improper manner. For example, in one case it was held improper for investigators to enter a man's home under false pretenses and then use a concealed camera to photograph him.

Cellphones and other devices that are equipped to track location using Global Positioning System (GPS) satellites are another new area of concern. Privacy experts warn that employees may not realize how much they can be tracked, especially if they use a cellphone or company vehicle with GPS on personal time.

Questioning Employees

The U.S. Supreme Court has said it is a violation of the First Amendment right of freedom of speech to force employees to admit wrongdoing by threatening to fire them. A forced confession "is the antithesis of free choice to speak out or to remain silent."

In addition to forcing confessions, courts in many states have held these situations are outrageous conduct and invasion of privacy:

In Arkansas, an employee was interrogated for six hours by company officials who berated her, accused her of sexual improprieties and would not allow her to eat, smoke or defend herself against the accusations.

In Colorado, an exemplary 20-year-old employee was questioned in a small room for over two hours by a manager who yelled at her, made her cry, and repeatedly accused her of theft despite her repeated denials.

In Vermont, an employee was fired after he was coerced into signing a confession by being kept in a meeting for three hours without a break.

> ***practical pointers:*** When questioning an employee, never make threats, such as "If you don't confess, you'll be fired." At the same time, don't make promises of leniency or other favors if the employee cooperates.
>
> The purpose of questioning a worker is to get information. The disciplinary action that may result from your investigation is a separate matter. It's best if the person questioning employees is not in a position to make the decision to terminate or discipline them.
>
> There should never be a show of force. A normal speaking tone should be used.
>
> Have a witness, and if the employee agrees, tape the meeting. This will avoid later questions of who is telling the truth about what happened during the meeting.
>
> A confession or other statement should be written by the employee, in his or her handwriting. Preparing a statement for the employee to sign smacks of coercion.
>
> The room in which the interrogation is conducted should not be small, hot or cold. It should have normal lighting. Tell the employee he or she can leave at any time and offer frequent breaks.

Wrongful Termination

When it is an illegal invasion of privacy to collect information, an employee who is fired for refusing to go along with it may be able to sue for wrongful termination in addition to invasion of privacy.

A California employer required all employees to take a pupillary reaction eye test for drugs. The test involved shining a light in the employee's eyes and watching the reaction. If the pupils dilate, then the employee is considered possibly under the influence of drugs and is sent for urinalysis.

In California, random drug tests of current employees in non-sensitive positions are illegal. In this case, the employee refused to allow the employer to shine the light in his eyes. He was terminated. The court held this was an invasion of privacy and wrongful termination.

It is also a wrongful termination where the employee is fired for refusing to violate another person's privacy. For example, a Maryland apartment manager was asked by his boss to enter tenants' apartments without their permission and to search their papers for phone numbers, salary records, and other private information. He refused and was fired. He was allowed to sue for wrongful termination.

Free Speech

The U.S. Constitution and all 50 state constitutions have provisions guaranteeing free speech. This is the principle that employees can't be discriminated against for what they say, nor can they be forced to support something against their will. To date, the courts have held these Constitutional provisions apply only to government employees, or in a few rare cases, to private-sector employees in highly regulated industries.

Connecticut has a statute that guarantees free speech in the workplace. It applies to any employer, government or not, who disciplines or discharges an employee for exercising free speech. But, the Connecticut courts have limited this protection to employees who speak out on matters of public interest.

The U. S. Supreme Court has held that the Republican Party cannot force its own employees to belong to the party in order to be hired, promoted or transferred. That would have a chilling effect on employees' freedom of speech and association.

In a singular Pennsylvania case, an insurance company employee was terminated because he refused to lobby for a no-fault law favored by his employer. This was held to be an invasion of his privacy and freedom of speech. But later Pennsylvania decisions have disavowed the decision by this court.

In another case, an employee of the U.S. Postal Service reported mail violations to her congressman. When the congressman asked the post office about her charges, the post office told him she also had filed a sex discrimination claim with the E.E.O.C. This was held a violation of her privacy rights.

What are the limits of free speech? In the case of government employees, the courts have distinguished between speaking on matters of public interest, versus speaking on matters of private concern. Comment on public issues is protected. But if I speak up about my paycheck, my disputes with the boss or other personal issues, my speech is not protected.

Employers may restrict employees if their speech substantially interferes with their job performance or their working relationships. But this must be proven, not assumed. That's why the Texas woman who worked for the sheriff couldn't be fired for her remark about shooting President Reagan. It was a matter of public interest and there was no evidence it caused disruption.

Arrest Record

Some states have statutes that prohibit employers from considering the fact that an employee has an arrest record. Other statutes allow considering convictions, although convictions of minor offenses may not be used.

The fact that an employee is arrested or even convicted of a crime while employed may not be relevant to the job. If not, using that private fact about them to take an adverse employment action may be invasion of privacy.

Arlene Golden was a high school guidance counselor in West Virginia. She was shopping at a local mall when she learned her daughter had wrecked her car. Mrs. Golden hurriedly left the store, unconsciously putting some items in her purse as she did. She was stopped and arrested for shoplifting. She pleaded no contest and was fined $100 for petty theft. She was then terminated by the school board for "a serious act of immorality."

The court held that a misdemeanor conviction by itself was not immoral. The court said the employer must show there is a relationship between the arrest and the job duties. In this case, she couldn't be fired unless her conduct indicated she was unfit to be a counselor. Or her behavior must have impaired or threatened the welfare of the school community because it had become the subject of notoriety.

Even where there is publicity about an arrest and conviction, there still may not be sufficient notoriety to justify termination. In a West Virginia case, a substitute teacher was found guilty of illegal possession of marijuana in his home. This was held not sufficiently job-related to justify his termination even though the charges were publicized.

In contrast, if the arrest is specifically related to the job, the employer may be justified in terminating on that basis. For example, UPS terminated a driver who was charged with theft while making a delivery to a UPS customer. He was arrested but freed pending trial.

The driver was questioned by his superiors about the incident. Based on his responses, he was terminated. Later, he was acquitted of the criminal charges and applied for reinstatement. UPS refused to rehire him. A Pennsylvania court upheld the company. Given the sensitive nature of UPS delivery jobs, the company had a legitimate interest in maintaining even the appearance of honesty among its employees.

Defamation

Defamation is the general term for any untrue statement which injures the reputation of a person. Written lies are called libel; spoken untruths are slander.

If you tell your boss about an employee's poor work performance so you can get advice on how to handle the problem, anything you say is probably "privileged." That means you can't be sued, even for lying, if you limit your comments to people who need to know, and discuss only the employee's work performance.

Comments made about an employee's work performance to people who don't need to know (co-workers, for example) may lead to a defamation claim. In 2003, a state appellate court found that a government employee's constitutional right of privacy was violated because the supervisor's announcement of the employee's reprimand to everyone went beyond the norm of acceptable employer conduct.

Comments about an employee's personal life - made to anyone - are likely to result in a lawsuit.

False Light

False light invasion of privacy is like defamation, but the two are not identical. Whereas defamation is an untrue statement, false light usually consists of actions that are interpreted to injure the reputation of the victim.

For example, when Merrill Lynch terminated a trader on the Chicago Board of Trade, they put him in a false light. Management made a surprise visit to his office, refused to allow him to speak to his staff, prevented him from taking all his personal belongings, and escorted him out of the building. They interrogated employees and others about entries in his travel and entertainment expense account. All of these actions implied that he was terminated for gross misconduct, when in fact he was not. An Illinois court held he was put in a false light.

Appropriation

Appropriation is using someone else's name or picture without their permission.

A Vermont employer put an employee's name and picture in a newspaper ad with the words, "it has been exciting and reassuring to know that Continental continues to expand its equipment and services to meet its obligation to serve you." Because she had never said this, it was held invasion of privacy by appropriation.

Medical Information

Medical information and employee medical records are "classically a private interest." They are protected under the common law in almost every state. The Americans with Disabilities Act says you must keep employee medical records separate from other employment information. Some states, such as California, also have statutes protecting the confidentiality of medical information.

The sweeping medical privacy regulations issued under the Health Insurance Portability and Accountability Act (HIPAA) went into effect for healthcare providers and group health plans in 2003 and 2004. Most of HIPAA's burdens fall on physicians, dentists, hospitals, and insurance companies. If you work in one of those capacities, you need detailed information about HIPAA, which is beyond the scope of this work. But if

you are an employer in a non-medical field, do you have obligations under HIPAA? Yes.

Employers receive health information about their employees in connection with the Family and Medical Leave Act (FMLA), the Americans with Disabilities Act (ADA), state disability, workers compensation, pre-employment physicals, fitness-for-duty examinations, accidents, and requests for sick leave. Health information you receive may include information about treatment for mental illness, dental and vision care, and prescription drug use.

You should always treat health information with strict privacy, because even if HIPAA does not apply, every state protects privacy to some extent. Historically, health information is considered to be extremely confidential. The biggest change HIPAA makes to existing law in most states is the requirement to give out a written notice of the person's privacy rights.

If the health information you receive is in connection with an "employment-related purpose" the information is NOT covered under HIPAA. Thus, when an employee applies for a medical leave of absence, that is an employment related purpose and not covered by HIPAA, and there is no requirement to give a written notice. But the health information may be protected by the FMLA, ADA or other statutes, and must be held in strict confidence.

Employers must give HIPAA notices and protect privacy only if the medical information they receive relates to "benefit payments" or "eligibility for coverage." For example, if employees are injured at work, they are entitled to workers compensation. Some companies augment the workers comp payments, and thus staff in Human Resources may become aware of the employee's health information in connection with "benefit payments." Or there may be some question as to whether the employee is eligible for workers compensation - perhaps the employer believes the employee was not injured at work. During the course of the ensuing investigation, the employee's manager may become aware of health information related to eligibility for coverage.

In these and other cases, the prudent employer will give employees the notice of privacy rights under HIPAA.

> ***practical pointer*:** Whether or not HIPAA is part of your life, now is a good time to go through your working files and make sure you do not have any unnecessary health information. If you must keep worker health information, review your privacy procedures and

ensure the information is kept locked up or in password-protected files.

Courts in some states, such as Oklahoma, follow the old rule that an employee cannot sue for invasion of privacy unless the confidential information is publicized to a large number of people. But the trend is to protect employees' medical information from being disclosed to even one person.

Medical information comes to the attention of managers in a number of ways. Employees often volunteer it in the course of calling in sick, requesting a leave of absence, or asking for light duty work. But just because they tell you, doesn't mean you can tell anyone else, unless that other person has a legitimate need to know.

If you promise to keep medical information confidential, you have a duty to do so. For example, an Illinois employee told the company nurse that she had undergone a mastectomy. The nurse promised she would keep the information confidential, but later revealed it to one other employee. The court held the company could be liable for invasion of privacy.

Even when the information is very sensitive, it may be revealed to protect the safety of others. In one case, an employee was diagnosed as suicidal and homicidal and potentially dangerous to other employees. His supervisor told his union representative. The West Virginia court held that communicating the information was in the interest of the employer and employees and was therefore not an invasion of privacy.

Even if employees' safety is not directly threatened, the employer may have a legitimate reason for revealing medical information. A Massachusetts supervisor sent a memo to personnel, revealing an employee had been diagnosed by the company doctor as paranoid. This was held not to be an invasion of privacy because management needed the information in order to evaluate the employee's ability to continue working.

In another case, a woman who worked in a Mississippi nuclear power plant fainted while doing decontamination work. Her co-workers were concerned she had radiation sickness, and were afraid they might become ill, too. The supervisor told them the co-worker had not fainted because of radiation, but because of a recent hysterectomy. This was held not to be an invasion of privacy because the co-workers had a legitimate interest in the information.

If employees don't guard their own medical information, it is no longer confidential and can be revealed to others. In a recent Kansas case, a woman told seven friends she was entering a drug and alcohol treatment center. She did not ask them to keep the information confidential. She also told her supervisor he could "tell anyone who asked." The company then sent a memo to 110 employees informing them of her treatment. This was held not to be an invasion of privacy because it was no longer a private fact.

Employers often have a legitimate reason to inquire about an employee's medical condition. Before you ask a doctor to tell you about an employee's medical condition, you may need a release. This is an agreement signed by the employee authorizing you to talk to the doctor.

There is a split among courts about whether a release is needed for an employer to talk about an employee with the *company* doctor or nurse. In a Massachusetts case, a release was not required. In Ohio, a release has been held necessary.

You must get releases from employees before you can contact their own doctors. Once you have a release, you must scrupulously follow its terms.

An Oregon case demonstrates how narrowly courts construe medical releases. An employee allowed her psychiatrist to write a letter to her employer stating she needed a two week medical leave due to severe anxiety neurosis. The company's employee assistance plan representative then met with the psychiatrist to follow up, asking if the employee would be able to continue her employment. The court held this was invasion of privacy, because the employee had not authorized the follow-up visit.

Information given by an employee to a counselor or doctor who is part of the company's Employee Assistance Program (EAP) is confidential and can't be revealed to the employer.

Requiring Medical Exams

Pre-employment medical exams are allowed under the law to ensure applicants are fit for duty. Under the Americans with Disabilities Act, a medical examination cannot be required before an offer of employment is made. Instead, you make an employment offer contingent on the applicant passing the medical exam.

The doctor who conducts the examination should have an accurate job description. Better still, the doctor actually should see the work performed in jobs that are physically demanding.

The doctor will be able to ask detailed questions about the applicant's medical history that would be illegal if asked by the company. But the doctor's report should not reveal this information to the company. Instead, it should state the applicant is able to work, unable to work, or able to work with restrictions.

The restrictions should be spelled out but not, in most cases, the reasons for the restrictions. For example, if an applicant can't lift more than 30 pounds due to a bad back, the report should merely state, "no lifting over 30 pounds."

In the case of applicants who are disabled, the doctor can reveal information to the employer which would be necessary to know in case of an emergency.

Psychological exams also are allowed in order to determine fitness for duty. These are allowed both before hiring or after employment begins, if there is a reasonable belief that an employee poses a hazard to a safe and healthy work environment. As with physicals, the psychotherapist's report should state only that the individual is able to work, unable to work, or able to work with restrictions.

Personnel Files and Information

In response to the events of September 11, 2001, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act of 2001. (USA PATRIOT Act) As part of an investigation of suspected terrorist activity, the Act allows the FBI to get an order from a judge requiring any employer to provide information such as dates of employment, address, and telephone number. The FBI can also get an order requiring production of employee voice mail, and can ask for permission to monitor an employee's voice mail or e-mail in real time. An employer that receives such a court order or request cannot disclose to anyone, including the employee, the fact the FBI is seeking information.

A federal law known as the Privacy Act limits the type of information federal agencies, the military and government corporations may maintain on their employees. In an effort to prevent identity theft, California has imposed substantial limitations on how employees' social security numbers may be used.

35 states have laws about personnel files. Most require employers to give employees access to their own files within a reasonable time after they request it -- usually within 7 days. These statutes generally apply both to employees and former employees.

Michigan and Pennsylvania allow employees to correct inaccurate information contained in their files. New Hampshire allows employees to copy their entire file; California employees are entitled only to copies of documents they sign.

Several states protect the privacy of other people who are mentioned in employees' personnel files. For example, Delaware allows companies not to give employees copies of letters of reference and reports of criminal investigations.

Wisconsin allows employers to keep confidential business information contained in personnel files if it relates to staff management planning (e.g. comparative rankings of employees, staffing projections).

As a manager, you may look into an employee's personnel file if you have a legitimate business reason. You may need to look at the last performance appraisal to measure progress over the year. You may have to check attendance records or vacation time accrued.

While looking for legitimate information, you might inadvertently see private information. An employee's claim for Workers' Compensation includes medical information. A request for insurance benefits for an employee, spouse or dependent may contain confidential information. You should not read this confidential information and you should not reveal it to others.

An employer must be cautious about revealing to other employees the reason employees have been terminated. They have a right to privacy. But employers often want to publicize why employees have been terminated so other employees will know that the company's rules are enforced.

A Wisconsin employer printed in the company newsletter the names of employees leaving employment and the reasons for their terminations. Included were such damaging reasons as "falsification of application." The court allowed it, saying the employer had a legitimate interest in letting employees know why a co-worker was no longer employed.

But the company can't announce it to people who have no reason to know. A California employer posted the reasons for an employee's termination in a public place that could be seen not only by co-workers, but also members of the general public. This was held to be invasion of privacy.

> ***practical pointers:*** An employee's personnel file should be kept locked up. Personnel files should be restricted to employees who have a need to see them. Medical information, including Workers' Compensation claims, insurance forms, and the like, should be kept in a separate file.
>
> You should not send copies of the entire personnel file to outsiders. For example, your Workers' Compensation carrier might ask for the personnel file to investigate an employee's past claims history. You should only give them information relevant to their investigation. There is a lot of information in files that isn't relevant, such as performance appraisals, disciplinary warnings and requests for (unrelated) sick days.

Some supervisors keep a working file on employees with brief documentation of events that haven't resulted in any action. You can't hide documentation that you've used to make a decision. Your back-up documentation for a warning should be in the official personnel file. But ongoing documentation that hasn't resulted in a poor performance appraisal, warning, demotion or other adverse employment decision generally can be kept separately and need not be shown to the employee. However, it is not a good idea to keep draft documents once you're finished. Throw out or shred drafts.

Home Address & Phone

A person's home address would seem to be very private. However, courts routinely have allowed employers to disclose the names and addresses of their employees to labor unions who are attempting to organize their workers. This is not usually an invasion of privacy because name and address are not considered a private matter.

However, it also may depend on who requests the address. We would expect the employer not to give information to others without inquiring into whether they have a legitimate need for the information.

The Oregon Supreme Court held it was an invasion of privacy to give out a home address where the individual specifically had requested it not be, because she was being harassed. The court said this was personal

information, which it defined as information which normally "would not be shared with strangers."

Home phone number has been held private by a court in Illinois.

Asking Personal Questions

Merely asking personal questions has been held to be invasion of privacy.

The Alabama Supreme Court found invasion of privacy in a case where a woman janitor was sexually harassed by the owner of the company. Within a few weeks of starting her job, he called her into his office and asked how she was getting along with her husband. A few days later, he again called her into his office, locked the door, and asked her how often and in what positions she and her husband had sex.

He continued this intrusive interrogation for weeks, and finally demanded she have oral sex with him. She sued for sexual harassment. She also sued for invasion of privacy. The court held it was invasion of privacy merely to be asked the questions. The fact that she didn't answer them did not make them any less intrusive.

Many courts have held that law enforcement and other government employees can't be forced to reveal personal information. Questions to police officers about personal and family history and sexual history have been held to invade privacy.

Certain psychological tests—most notably the Minnesota Multiphasic Personality Inventory, the most commonly-used psychological test in the U.S.—have been held to be invasions of employee privacy when used by certain employers. In 2000, Rent-A-Center agreed to settle a class action by paying nearly $2 million to employees and applicants who challenged the test, which asked questions about their sex lives and religious beliefs.

Relationship Restrictions

The courts have protected the right of government employees to enjoy freedom in their relationships.

The U.S. Supreme Court has held it was an invasion of privacy to dismiss a teacher who was getting a divorce. Other courts have said police officers and presumably other government employees cannot be dismissed for these reasons:

dating the daughter of a known mobster,
having an affair with another police officer in the past,
living together without being married, and
living with an 18 year-old woman.

In a few cases, courts have upheld dismissals that were rationally related to legitimate government interests. For example, a rule prohibiting police officers from living with each other was held reasonable to maintain the discipline necessary in a quasi-military unit.

A Pennsylvania court allowed termination of a bail commissioner because his wife became a political party ward. This was justified by the compelling state interest for the bail commissioner to avoid even the appearance of partisanship. Anti-nepotism polices in school systems, hospitals, and other public employers have been upheld by various federal courts, which found that there were legitimate concerns about preventing favoritism, discipline problems, friction and disharmony.

Historically, non-government employees have received much less protection. Companies have been allowed to dismiss employees for these reasons:

having extra-marital affairs
attending a business convention with someone not a spouse
becoming engaged to be married
dating co-workers.

But despite these cases, the recent trend is to expand employees' relationship rights.

The leading case in the country is California's *Rulon-Miller v. IBM*. In this case, a saleswoman in the typewriter division was fired for dating a man who worked for a competitor of IBM computers. She did not have access to IBM trade secrets, and there was no evidence she was giving him any confidential information. In fact, he played on the IBM softball team, so he knew many IBM employees.

IBM had a written policy expressly guaranteeing employees the right to privacy. The policy provided in part,

"We have concern with an employee's off-the-job behavior only when it reduces his ability to perform regular job assignments, interferes with the job performance of other employees, or if his outside behavior affects the reputation of the company in a major way. . . . Action should be taken only when a legitimate interest of

> the company is injured or jeopardized. Furthermore, the damage must be clear beyond a reasonable doubt. . . ."

The court held that Rulon-Miller had a privacy right to date who she wished as long as it was not to the detriment of IBM.

Similarly, a New Jersey court held that an employee could not be fired as a result of extramarital sexual activities if the company would have to intrude upon his privacy in order to enforce its rule prohibiting affairs.

Courts also have found invasion of privacy where employees have been harassed for interracial relationships. An Indiana court held this because of the strong public policy against racial discrimination.

While most states have statutes prohibiting discrimination based on marital status, there is a split of authority as to whether "marital status" includes not only decisions made because someone is single, married, separated, widowed, or divorced, but also actions based on the identity of an employee's spouse. Only three states, Minnesota, North Dakota, and Oregon, legislatively prohibit discrimination base on the identity of the spouse. Courts in Hawai'i and Montana have interpreted their anti-discrimination laws to find unlawful action where an employee would not have been fired but for marriage to a co-worker.

Lawful Activities

Do you have the right to bungee-jump or sky-dive? Four states—California, Colorado, New York and North Dakota—have laws barring employers from discriminating against employees because of lawful off-duty activities. These were passed in response to employers' attempts to impose lifestyle restrictions on their workers.

And, more than half the state legislatures have said that employers can't refuse to hire or otherwise discriminate against employees or applicants who use tobacco or alcohol. Of course, employers are still free to have and enforce policies against drinking or smoking on the job, and against being under the influence of drugs or alcohol at work. Seven states protect employees who use any legal substance off-duty.

Appearance Standards

Establishing appearance standards or dress codes have long been held to be the right of the employer. Today, in some localities, this historic right is being challenged.

The general rule still is that employers have the right to set appearance standards. Dress codes have been upheld that require employees to "achieve the Brooks Brothers look" as long as it was applied to men and women equally.

Dress codes have been struck down by courts where they are discriminatory. In one case, a retail store allowed male sales clerks to wear street clothes, but required female sales clerks to wear uniform smocks over their clothes. The court held this was illegal sex discrimination.

But simply having different requirements for men and women is not necessarily sex discrimination. Courts recognize that in the professional world, women wear earrings and men don't. Men wear pants and women wear skirts. Men wear neckties and women don't. These distinctions have not been held to be discriminatory, because they do not put an undue burden on either sex. But, California has a law on the books that women can't be required to wear skirts.

In 1990, an Oregon court allowed a company to fire a male employee for refusing to take off an earring, even though women were allowed to wear them.

A schoolteacher who was fired for wearing short skirts lost her case. The court held the school had administrative reasons that made the dress code necessary. A woman who wore tank tops to work could be fired for wearing provocative clothes.

A woman attorney couldn't complain of sex discrimination when her boss said she dressed "too flashy" and should tone down her style, because male attorneys probably were given similar advice.

In line with these cases, the U.S. Supreme Court came to a similar result when it ruled on appearance standards in a 1990 case. Ann Hopkins was an associate accountant at Price Waterhouse. Of the 88 people in her class at PW, she was ranked number one in terms of performance. Despite that, she was one of the few who was not offered a partnership.

Among the reasons given were that she didn't act femininely. In finding that Ms. Hopkins had been discriminated against, the Supreme Court noted it was unlikely that any man had been denied partnership on this basis. However, if the employer had said she didn't look "professional," perhaps the result would have been different.

Hair and beard regulations also have had mixed success. Short hair for men has been upheld for the military, including reservists. An airline was

allowed to prohibit employees from wearing cornrows. But teachers in Mississippi successfully challenged hair and beard regulations, on the theory that they were not reasonably related to the job. And remember that employee religious beliefs or medical conditions may entitle them to exemption from rules on facial hair and headgear.

Washington, D.C. and Howard County, Maryland, have ordinances that prohibit discrimination on the basis of physical appearance. These ordinances allow employers to have dress codes for legitimate business reasons but prohibit them from applying their dress codes inconsistently.

Damages

If an employee's privacy is invaded, what are the available damages? Although the law does not protect the "neurotically thin-skinned," there does not have to be any economic loss, or even any discovery of private information, for employees to win damages.

They don't have to show they were embarrassed or suffered emotional injury. It is enough that their privacy was invaded.

As a New Hampshire court put it, an invasion of privacy "impairs the mental peace and comfort of the individual and may produce suffering more acute than that produced by a mere bodily injury."

Privacy Principles

There are six general principles that will prevent invasion of privacy:

1. establish reasonable work standards and objectively measure employees against them,
2. advise employees in advance about what information is collected, why and how,
3. guarantee information will not be disseminated to outsiders without the employee's consent,
4. give employees access to records and opportunity to correct inaccuracies,
5. collect information only that is relevant to the job,
6. gather information in the least intrusive way possible.

Joseph R. Grodin is a former California Supreme Court justice who is a leading thinker in the field of privacy. He believes that privacy is a fundamental principle of U.S. law.

He says the U.S. Constitution is based on the idea that the individual surrenders to government only what is reasonably necessary in order to be governed. Similarly, employees should be required to give up only what is necessary for the employer to do business.

Privacy is precious. We should do all we can to protect the privacy of others. It is by protecting the privacy of others that we protect our own.