Part 3

Regulation of the Employment Environment

Chapter 14

The Employee's Right to Privacy and Management of Personal Information

Learning Objectives

When you finish this chapter, you should be able to:

- **LO1** Describe the nature of privacy as a fundamental right.
- **LO2** Explain the three general ways in which privacy is legally protected in the United States.
- **LO3** Define the legal concept of a "reasonable expectation of privacy" and its application to the workplace.
- **LO4** Identify and apply the standard for unreasonable searches and seizures under the Fourth Amendment.
- **LO5** Explain the distinctions between the protections for public- and private-sector privacy protections.
- **LO6** Describe the legal framework that applies to private-sector privacy cases.
- **LO7** Identify and differentiate the *prima facie* cases for common-law claims of privacy invasions (intrusion into seclusion, public disclosure of private facts, publication in a false light, and breach of contract/defamation).
- **LO8** Explain the extent to which an employer can legally dictate the off-work acts of its employees.

LO9 Discuss how advances in technology have impacted employee privacy.

LO10 State the key business justifications for employee monitoring.

LO11 Explain the most effective means by which to design and to implement a technology use policy.

LO12 Describe the legal environment that surrounds employee use of social media technologies.

Opening Scenarios

SCENARIO 1

1 Scenario

Aravinda has been reading in the news lately of the skyrocketing costs of health care, particularly surrounding the HIV epidemic. She is concerned that her small 10-employee company would suffer a financial disaster if one of its workers contracted the virus since the company's insurance costs would increase. Therefore, she wants to conduct a confidential HIV test of each present employee and future applicant. Aravinda has several concerns. First, what if an individual refuses to take the test based on the grounds of invasion of privacy? Second, if someone tests positive, can Aravinda refuse to hire or can she discharge her or him without violating federal law protecting employees with disabilities? Third, how can she otherwise protect against rising costs? Fourth, if an employee tests negative, but Aravinda decides to terminate the employee anyway, is she liable for the *appearance* that the employee is HIV-positive and that Aravinda terminated her or him as a consequence of the test results? How can she ensure that the test results are kept confidential?

SCENARIO 2

2 Scenario

Abraham, a real estate agent, has three children, two of whom are in college. In order to earn extra money to help with college tuition payments, Abraham (who studied modern dance during his college career) finds a job dancing in a club that caters specifically to women. While not exactly erotic dancing (he keeps all of his clothes on), it is not ballroom dancing either. Celebrating during a bachelorette party, one of the partners of the real estate firm for which Abraham works catches sight of him dancing. When he arrives at the office the next day, she calls him into her office and orders him to quit his night job. She claims that both clients and potential clients might see him there and he would lose all credibility as a real estate agent. Does she have a right to require Abraham to do this as a condition of future employment? (Presume that he is an employee and not an independent contractor.)

SCENARIO 3

3 Scenario

Solange receives a spam e-mail asking her to go look at a certain Web site. Since she does not know who it is from or why she is receiving it, she clicks on the link and finds herself at a Web site devoted to XXX-rated videos. She is so perturbed by this occurrence that she spends a few moments looking around the Web site trying to find its site administrator. She intends to send off a message to the administrator asking this person not to send her any more junk mail. After searching for several minutes with no luck, she leaves the Web site and goes back to reading her e-mail. A few days later, she is called into her manager's office and reprimanded for using employer-owned computer equipment for personal interests such as this XXX-rated video site. It seems that her manager was using a program that alerted him any time an employee perused certain inappropriate Web sites. She tries to explain but leaves with a written reprimand in her hand and a copy in her files. She is furious, not only at her manager's unwillingness to understand, but also at the invasion of her privacy posed by this computer monitoring. Does her employer have a right to monitor her computer use in this way?

Are There Guarantees in Life?

Privacy is a surprisingly vague and disputed value in contemporary society. With the tremendous increase in computer technology in recent decades, calls for greater protection of privacy have increased. Yet, there is widespread confusion concerning the nature, extent, and value of privacy. Philosophers have argued that our society cannot maintain its core values without simultaneously guaranteeing the privacy of the individual. Edward Bloustein writes that "an individual deprived

of privacy merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual."[1]

Recent inventions and business methods call attention to the next step that must be taken for the protection of the person and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[2]

Philosopher Chris MacDonald explains that privacy is about having a realm of personal control from which others can be excluded at will. In other words, it has to do with freedom of action, freedom from the prying eyes of neighbors, governments, or employers. The more such freedom we have, the more privacy we have.[3]

Europeans generally view employee rights using a different perspective from that in the U.S. While Americans view rights of employees in terms of the protection of their privacy, Europeans are more likely to perceive their protection with regard to human dignity, the employee's right to be free from embarrassment and humiliation.[4] The result of this distinction is that European employees generally enjoy a wider range of freedom from employer intrusion in the workplace than do U.S. employees. Indeed, some U.S. firms that engage in business internationally have found themselves in violation of EU standards, and subject to hefty fines, when they applied their privacy rules to employees who were located in the EU.

LO1

The concept of privacy as a fundamental right is certainly not limited to the United States and Europe. Privacy is protected in the Qur'an[5] and was recognized by Mohammed.[6] Ancient Greece already had laws protecting privacy, and the Jewish Talmud considers privacy an aspect of one's sanctity, providing rules for protecting one's home. In fact, the Talmud contains reference to "harm caused by seeing" (*hezeq re'iyyah*) when one intrudes upon another.

But do employees actually have a "fundamental right to privacy" as many believe? The answer to this question is not as easy as one might presume, given the wide recognition of employee rights in the workplace. The right to privacy may not be as fundamental as employees generally believe it to be, which makes it all the more important in these days of advancing information technology. Computer technology, though largely beneficial, can have a negative effect on employees if the easily obtained information is misused, incorrect, or misleading. Employers now have a greater capacity to invade an employee's privacy than ever before. Among other devices, there are chairs that can sense and record the time an employee spends at his or her desk, computer programs that measure employees' computer keystrokes to ensure they are as productive as they should be, phones that monitor employees' phone calls, and policies related to workplace communication to make sure all communications are work-related. Monitoring is only increasing in power, ability, and frequency. Sales of computer monitoring and

surveillance software have increased almost 500 percent to $622 million in 2006.[7] But perhaps there is presently a greater employer need for seemingly private information, with more than 75 percent of 14.8 million drug users in the United States employed.[8] Drug use in American industry costs employers approximately $82 billion per year in overall productivity due to absenteeism and attrition; theft of employer property by employees is estimated at $10 billion per year; and failure to perform an intensive reference and background check of an applicant may cost the employer enormous amounts in litigation fees defending claims of negligent hiring, easily outweighing the cost of a drug test, usually less than $50. In this time of increased competition in the global marketplace, each employee becomes all the more crucial to the workings of the company. An employer has a justified basis for attempting to choose the most appropriate and qualified person for the job; the means by which the employer obtains that information, however, may be suspect.

The right to privacy is not only balanced with the arguably legitimate interests of the employer but also with the employer's responsibility to *protect* the employees' personal information. A 2007 study of more than 800 North American privacy and security professionals reported that there is a strong likelihood of a security breach relating to personally identifiable information. In fact, 85 percent of those responding had experienced or observed a security breach within the past 12 months and 63 percent had experienced multiple breaches during that time—between 6 and 20 occurrences.[9]

Since erosion of at-will employment was the dominant issue of the 1980s, scholars have predicted that privacy will be the main theme for the 1990s and beyond. This chapter will address the employee's rights regarding personal information and the employer's responsibilities regarding that information, as well as the employer's right to find out both job-related and nonrelated personal information about its employees. Chapter 3 previously addressed other issues regarding the legality of information gathering through testing procedures. This chapter will not address issues relating to consumer privacy since they fall outside the scope of the chapter's and the text's primary focus.

Background

LO2

There are three ways in which privacy may be legally protected: by the Constitution (federal or state), by federal and/or state statutes, and by the common law. The U.S. Constitution does not actually speak of privacy, but privacy has been inferred as a necessary adjunct of other constitutional rights we hold. The right to privacy was first recognized by the Supreme Court in *Griswold v. Connecticut,*[10] when the Court held that a Connecticut statute restricting a married couple's use of birth control devices unconstitutionally infringed on the right to marital privacy.

fundamental right
A right that is guaranteed by the Constitution, whether stated or not.

The Court held a constitutional guarantee of various zones of privacy as a part of the **fundamental rights** guaranteed by the Constitution, such as the right to free speech and the right to be free from unreasonable searches and seizures. The latter right is that on which many claims for privacy rights are based; the Court

Exhibit 14.1 *Realities about Employee Privacy Rights*

1. Employees do not have an absolute right to privacy in their workplace.
2. It is not a breach of an employee's right to privacy for an employer to ask with whom the employee lives.
3. In the private sector, the Constitution does not protect employees' right to be free from unreasonable searches and seizures.
4. Without constitutional protection, employees are safe guarded to some extent by common law protections against invasions of privacy.
5. Though an employee may give information to an employer, the employer is still bound to use that information only for the purpose for which it was collected.

has held that under certain circumstances the required disclosure of certain types of personal information should be considered an unreasonable search. It has protected against the mandatory disclosure of personal papers, and it decided in favor of the right to make procreation decisions privately.

While baseless or unjustified intrusions, at first blush, may appear to be completely abhorrent in our society, proponents of the argument that employers can ask whatever they please argue that if an employee does not want to offer a piece of information, there is something the employee is trying to hide. For example, why would an employee refuse to submit to a drug test if that employee is not abusing drugs? Do **private-sector** employers have the right to ask their employees any question they choose and take adverse employment actions against the employee if she or he refuses to answer since they are not necessarily constrained by constitutional protections? (See Exhibit 14.1, "Realities about Employee Privacy Rights.")

private sector
That segment of the workforce represented by private companies (companies that are not owned or managed by the government or one of its agencies).

Additionally, employees are concerned about the type of information gathered in the course of applying for and holding a job. Who has access to that information? What information may be deemed "confidential," and what does that mean to the employee? Evidently, employers perceive challenging issues among these and others with regard to privacy; as of 2004, there were more than 2,000 chief privacy officers (CPOs) in businesses around the world, more than 10 times the estimate three years ago.[11]

Workplace Privacy, Generally

LO3

Privacy protections in the workplace are a completely different animal than other types of workplace protections, such as those against discrimination on the basis of gender, disability, and age. Simply put, employees in the private sector workplace do not have broad rights to personal privacy. Why? To begin, unlike the other areas, no *comprehensive* federal workplace privacy legislation exists. The protections that do exist, as discussed previously, arise from a motley collection of inferences from the Constitution, limited-purpose federal laws, assorted state laws, and some **common law** (court-created through case law).

common law
Law made and applied by judges, based on precedent (prior case law).

Second, in almost every state, employees are hired at will, which means that employers can fire them for good reasons, for bad reasons, or for no reason at all (but not for an illegal reason), as we shall discuss in more detail later. If an employer legitimately can fire an employee for "bad reasons," you can see quite clearly why an employee is not going to be successful in stating a case against the employer for violating the employee's privacy unless the employee can fit his or her complaint specifically into one of the protections guaranteed by the federal, state, and common laws, thus turning a "bad reason" into an "illegal reason."

Perhaps the most effective way to understand workplace privacy protections is to examine where the protections do exist. Courts have recognized an employee's right to privacy in the workplace where there is a "reasonable expectation of privacy."[12] However, they have also held that a work area, unlike, for instance, a bedroom, is not a place of solitude or seclusion; so, there is no expectation of privacy in that environment.[13] In addition, anything that the employer provides to employees—a telephone, computer, desk, chair, or other business-related instrument—contains no expectation of privacy because it belongs to the employer, not to the employees. Thus, the content of e-mails, telephone calls, and computer activity conducted on employer-provided equipment is not private.

Is there *any* reasonable expectation of privacy in the workplace? (See Exhibit 14.2, "'Reasonable' Areas in Which to Expect Privacy in the Workplace, Subject to Exceptions.") Yes, employees have an expectation of privacy with regard to their body, including what they carry in their pockets. Their employer generally does not have the right to frisk them or to require them to disclose what they are carrying in your pockets; although, as we shall see later, there are situations in which such as invasion of privacy would be appropriate. This expectation extends to company-provided bathrooms, changing rooms, and showers. But, should this expectation cover drug testing? We will explore that question later in this chapter.

Second, employees have an expectation of privacy in connection with items that are contained in other normally private locations, such as a purse or briefcase;

Exhibit 14.2 *"Reasonable" Areas in Which to Expect Privacy in the Workplace, Subject to Exceptions*

1. One's body and physical space; one has a reasonable expectation to be free from a pat-down or body search.
2. Normally private locations, such as a purse or briefcase.
3. Personal information, accessed without permission.

however, these locations, also, are subject to exceptions under certain circumstances. For example, if an employee puts a purse in a company-provided desk drawer, the employer generally has the right to examine the desk drawer but likely not the contents of their purse. Similarly, employees have an expectation of privacy in the contents of their car that sits in the company parking lot, assuming that it is not a company car or that they are not using the car for company purposes other than to go to and from work. Their employer generally cannot go and search their car, with some exceptions.

Third, they have an expectation of privacy in their personal (not personnel) records and information. For example, they have the right to assume that their employer has no right to access their credit history, their driving record, or their family's medical records without their permission; but, we can all imagine situations in which that rule may not apply or may be excepted. Their employer, for example, could reasonably expect to access their driving history if they were applying for a job operating a company vehicle, although the employer needs their permission to do so.

Finally, workers have an expectation of privacy in what they choose to do in their free time, when they are away from work. However, this expectation is not quite as extensive as one might anticipate. Plenty of employers have tried to restrict what employees do in their free time, some successfully.

While the list may seem broad, the scope of workplace privacy rights is actually quite limited. The vast majority of the time during which employees are present at their employers' offices, they are subject to monitoring and other intrusions. Employers are free to monitor their movements, the keystrokes they make on their employer-provided computers, and the time they spend communicating with coworkers. Technological improvements have not only made their task that much easier but have also generated new ideas for intruding on employee privacy never before imagined (iris scans, voice prints, and face geometry, to name three).

Now we shall examine the specifics, first exploring public sector employee privacy, then continuing to private sector employee privacy.

Public Sector Employee Privacy

public sector
That segment of the workforce represented by governmental employers and governmental agency employers. In some situations, this term may include federal contractors.

With regard to the **public sector**, the Constitution protects individuals from wrongful invasions by the state or by anyone acting on behalf of the government. The personal privacy of federal, state, and local employees is therefore protected from governmental intrusion and excess. As we will see later in this chapter, private-sector employees are subject to different—and often fewer—protections.

Constitutional Protection

The Fourth Amendment and Its Exceptions

For the Fourth Amendment's protection against unreasonable search and seizure to be applicable to a given situation, there must first exist a "search or seizure." The Supreme Court has liberally interpreted "search" to include a wide variety of activities such as the retrieval of blood samples and other bodily invasions,

including urinalyses, as well as the collection of other personal information. One might imagine how this umbrella gets wider as technology advances.

LO4

Case 1

For the search to violate the Fourth Amendment, that search must be deemed unreasonable, unjustified at its inception, and impermissible in scope. You will read in the seminal Supreme Court case, *O'Connor v. Ortega,* included at the end of the chapter, that a search is justified "at its inception" where the employer has reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or where the search is necessary for a noninvestigatory work-related purpose such as to retrieve a file.

It is critical to review the *O'Connor* case to understand both the fundamental basis of public-sector search and seizure law as it applies to the workplace as well as much of current case law today. The Court held that a search is permissible in scope where "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the misconduct being investigated."

Generally, all searches that are conducted without a judicially issued warrant based on a finding of reasonable cause are held to be unreasonable. But there are several exceptions to this rule, including searches that happen as part of an arrest, some automobile searches, pat-down searches with probable cause to believe the subject is armed, and administrative searches of certain regulated industries.

One example of an exception occurred in *Shoemaker v. Handel*[14] where the Supreme Court held that a drug-related urine test of jockeys without a warrant was acceptable because it satisfied the court's two-pronged test. The Court held that (1) where there is a strong state interest in conducting the unannounced warrantless search and (2) where the pervasive regulation of the industry reduces the expectation of privacy, the search does not violate the Fourth Amendment. Similarly, in *Skinner v. Railway Labor Executives Association,*[15] decided three years after *Shoemaker,* the Court again addressed the question of whether certain forms of drug and alcohol testing violate the Fourth Amendment. While this case is discussed in this text in connection with testing, it is relevant here for the Court's analysis of the privacy right challenged. In *Skinner,* the defendant justified testing railway workers based on safety concerns: "to prevent accidents and casualties in railroad operations that result from impairment of employees by alcohol or drugs." The Court held that "[t]he Government's interest in regulating the conduct of railroad employees to ensure safety, like its supervision of probationers or regulated industries, or its operation of a government office, school, or prison, likewise presents 'special needs' beyond normal law enforcement that may justify departures from the usual warrant and probable-cause requirements."

It was clear to the Court that the governmental interest in ensuring the safety of the traveling public and of the employees themselves "plainly justifies prohibiting covered employees from using alcohol or drugs on duty, or while subject to being called for duty." The issue then for the Court was whether the means by which the

defendant monitored compliance with this prohibition justified the privacy intrusion absent a warrant or individualized suspicion. In reviewing the justification, the Court focused on the fact that permission to dispense with warrants is strongest where "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search," and recognized that "alcohol and other drugs are eliminated from the bloodstream at a constant rate and blood and breath samples taken to measure whether these substances were in the bloodstream when a triggering event occurred must be obtained as soon as possible." In addition, the Court noted that the railway workers' expectations of privacy in this industry are diminished given its high scrutiny through regulation to ensure safety. The Court therefore concluded that the railway's compelling interests outweigh privacy concerns since the proposed testing "is not an undue infringement on the justifiable expectations of privacy of covered employees." Consider the possible implications of this and related decisions on genetic testing in governmental workplaces or in employment in heavily regulated industries such as that involved in *Skinner.*

Finally, the employer may wish to conduct a search of employee lockers. Would this be acceptable? Under what circumstances is an employer allowed to conduct searches? A search may constitute an invasion of privacy, depending on the nature of the employer and the purpose of the search. The unreasonableness of a search is determined by balancing the extent of the invasion and the extent to which the employee should expect to have privacy in this area against the employer's interest in the security of its workplace, the productivity of its workers, and other job-related concerns.

Prior to any search of employer-owned property, such as desks or lockers, employees should be given formal written notice of the intent to search without their consent. Where the employer intends to search personal effects such as purses or wallets, employees should be forewarned, consent should be obtained prior to the search, and employees should be made well aware of the procedures involved.[16] Consent is recommended under these circumstances because an employee has a greater expectation of privacy in those personal areas. These rights are significantly diminished where the employer is not restrained by constitutional protections.

In an interesting combination of private/public workplace rights, the Ninth Circuit addressed these issues in the 2007 case, *United States v. Ziegler.*[17] In that case, Ziegler worked for a private company that had a clear policy in technology use. It explained that equipment and software were company-owned, to be used for business purposes only, and that employees' e-mails would be constantly monitored. The FBI received a complaint from the firm's Internet provider that Ziegler had accessed child pornography from a company computer and requested access to his computer.[18] The employer consented to the request. The court held that the *employer* had the right to consent to the search because the computer was workplace property and the contents of Ziegler's hard drive were work-related items that contained business information and that were provided to, or created by, the employee in the context of a business relationship. Ziegler's

downloading of personal items (pornography) did not destroy the employer's common authority over the computer given the company's policies that *informed employees that electronic devices were company-owned and subject to monitoring*—two key components necessary to the reasonable expectation element in any employment context.[19]

When an employee is detained during a search, the employer may have a claim for *false imprisonment,* which is defined as a total restraint on freedom to move against the employee's will, such as keeping an employee in one area of an office. The employee need not be "locked" into the confinement to be restrained; but when the employee remains free to leave at any time, there is no false imprisonment.

The Fifth and Fourteenth Amendments

The Fifth and Fourteenth Amendments also protect a government employee's right to privacy in that the state may not restrict one's rights unless it is justified. For instance, the Supreme Court has consistently held that everyone has a fundamental right to travel, free of government intervention. Where the state attempts to infringe on anything that has been determined to be a fundamental right, that infringement or restriction is subject to the *strict scrutiny* of the courts. For the restriction to be allowed, the state must show that the restriction is justified by a *compelling state interest.* Moreover, the restriction must be the least intrusive alternative available.

On the other hand, for those interests not deemed by the courts to constitute fundamental rights, a state may impose any restrictions that can be shown to be *rationally related to a valid state interest,* a much more lenient test.

To determine whether the state may restrict or intrude on an employee's privacy rights, it must first be determined whether the claimed right is fundamental. Two tests are used to make this determination. First, the court may look to whether the right is "implicit in the concept of ordered liberty, such that neither liberty nor justice would exist if [the rights] were sacrificed." Second is whether the right is "deeply rooted in this Nation's history and tradition."

While conception, child rearing, education, and marriage have been held to be within the area of privacy protected by the Constitution, other issues have not yet been addressed or determined by the Court, including the right to be free from mandatory preemployment medical tests. Moreover, the Court has found *no* general right of the individual to be left alone.

The Privacy Act of 1974

Governmental intrusion into the lives of federal employees is also restricted by the Privacy Act of 1974. Much of the discussion in the area of employee privacy is framed by governmental response to the issue, both because of limitations imposed on the government regarding privacy and because of the potential for abuse. The Privacy Act of 1974 regulates the release of personal information about federal employees by federal agencies. Specifically, but for 11 stated exceptions, no federal agency may release information about an employee that contains the

Exhibit 14.3 *Privacy Act of 1974*

PRIVACY ACT OF 1974

No Agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be

1. To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.
2. Required under section 552 of this title; (*the Freedom of Information Act*). (*Note that this act does not apply to "personnel, medical, and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."*)
3. Or a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section; (*a purpose that is specifically compatible with the purpose for which the information was gathered*).
4. To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity. . . .
5. To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.
6. To the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value.
7. To another federal agency or to an instrumentality of any government jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.
8. To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.
9. To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee or subcommittee of any such joint committee.
10. To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office.
11. Pursuant to the order of a court of competent jurisdiction.

means for identifying that employee without the employee's prior written consent. (See Exhibit 14.3, "Privacy Act of 1974.")

There are four basic principles that underlie the Privacy Act:

1. Employees should have access to their own personnel files, and there should be some way for them to find out the purposes for which the files are being used.
2. There should be some mechanism by which an employee may correct or amend an inaccurate record.

3. The employee should be able to prevent information from being inappropriately revealed or used without her or his consent, unless such disclosure is required by law.
4. The person who is in charge of maintaining the information must ensure that the files are not falling into the wrong hands and that the information contained within the files is accurate, reliable, and used for the correct reasons. By affording the employee with these rights, Congress has effectively put the right of disclosure of personal information in the hands of the employee, at least when none of the 11 specified exceptions applies.

When one of the Privacy Act exceptions applies, the act dismisses the employee consent requirement, which gives the agency total control over the use of the file. The right to privacy is not absolute; the extent of protection varies with the extent of the intrusion, and the interests of the employee are balanced against the interests of the employer. Basically, the information requested under either the Privacy Act or the Freedom of Information Act is subject to a balancing test weighing the need to know the information against the employee's privacy interest.

The Ninth Circuit Court of Appeals has developed guidelines to assist in this balancing test. The court directs that the following four factors be looked to in reaching a conclusion relating to disclosure:

1. The individual's interest in disclosure of the information sought.
2. The public interest in disclosure.
3. The degree of invasion of personal privacy.
4. Whether there are alternative means of getting the information.

Critics of the act suggest that it is enormously weakened as a result of one particular exemption that allows disclosure for "routine use" compatible with the reason the information was originally collected. In addition, certain specific agencies are exempted. For instance, in March 2003, the Department of Justice exempted the National Crime Information Center, which is a resource for 80,000 law enforcement agencies.

The Privacy Act grants employees two options for relief: criminal penalties and civil remedies, including damages and injunctive relief. The act also allows employees who are adversely affected by an agency's noncompliance to bring a civil suit against the agency in federal court.

Privacy Protection Study Commission

The Privacy Protection Study Commission was formed by Congress with the purpose of studying the possibility of extending the Privacy Act to the private sector. In 1977, the commission concluded that the Privacy Act should not be extended to private employers but that private-sector employees should be given many new privacy protections. The suggested protections required a determination of current information-gathering practices and their reasons, a limitation on the information that may be collected to what is relevant, a requirement that the employer inform its employees to ensure accuracy, and a limitation on the usage of the information gathered both internally and externally.

The commission further found that certain issues demanded federal intervention and, for this reason, recommended that (1) the use of polygraph tests in employment-related issues be prohibited; (2) pretext interviews be prohibited; (3) the use of arrest or criminal records in employment decisions be prohibited except where otherwise allowed or required by law; (4) employers be required to use reasonable care in selection of their investigating agencies; and (5) the Federal Fair Credit Reporting Act provisions be strengthened. These recommendations have yet to be implemented by Congress, primarily due to private employers' vocal rejection of such an extension of federal law due to the cost of the implementation of the recommendations.

Federal Wiretapping—Title III

Title III of the Federal Wiretap Act,[20] as amended (particularly by the Electronic Communications Privacy Act of 1986, discussed below), provides privacy protection for and governs the interception of oral, wire, and electronic communications. Title III covers all telephone communications regardless of the medium, except that it does not cover the radio portion of a cordless telephone communication that is transmitted between the handset and base unit. The law authorizes the interception of oral, wire, and electronic communications by investigative and law enforcement officers conducting criminal investigations pertaining to serious criminal offenses, or felonies, following the issuance of a court order by a judge. The Title III law authorizes the interception of particular criminal communications related to particular criminal offenses. In short, it authorizes the acquisition of evidence of crime. It does not authorize noncriminal intelligence gathering, nor does it authorize interceptions related to social or political views.

Forty-four states, plus the District of Columbia and the Virgin Islands, have statutes permitting interceptions by state and local law enforcement officers for certain types of criminal investigations.[21] All of the state statutes are based upon Title III, from which they derive. These statutes must be at least as restrictive as Title III, and in fact most are more restrictive in their requirements. In describing the legal requirements, we will focus on those of Title III since they define the baseline for all wiretaps performed by federal, state, and local law enforcement agencies. In recent years, state statutes have been modified to keep pace with rapid technological advances in telecommunications.

Wiretaps are limited to the crimes specified in Title III and state statutes. Most wiretaps are large undertakings, requiring a substantial use of resources. In 2009, the average cost of installing intercept devices and monitoring communications was more than $52,000, up 10 percent from the 2008 costs.

The frequency of wiretap requests is also growing. In 2009, the number of federal and state wiretaps grew by 26 percent; none of the 2,376 federal and state applications for a wiretap were denied.

Electronic Communications Privacy Act (ECPA)

Title III was created to combat invasion of the government for eavesdropping, in large part due to the Watergate scandal in the 1970s. Originally the federal

statutes targeted government eavesdropping on telephone discussion without the consent of the speakers. The federal statute required the government agents to obtain a warrant before they could intercept any oral discussions. In late 1986, Congress increased the coverage by broadening the range of electronic communications, resulting in the ECPA.

The ECPA covers all forms of digital communications, including transmissions of text and digitalized images, in addition to voice communications on the telephone. The law also prohibits unauthorized eavesdropping by all persons and businesses, not only by the government. However, courts have ruled that "interception" applies only to messages in transit and not to messages that have actually reached company computers. Therefore, the impact of the EPCA is to punish electronic monitoring only by third parties and not by employers. Moreover, the ECPA allows interception where consent has been granted. Therefore, a firm that secures employee consent to monitoring at the time of hire is immune from ECPA liability, which means that an employer does not violate the ECPA when it opens and reads employee e-mails on its own system.[22]

Private Sector Employee Privacy

LO5

Despite the fact that public and private employers have a similar legitimate need for information about applicants and employees to make informed decisions about hiring, promotion, security, discipline, and termination, privacy rights in the private sector of employment are limited; an employee who is arbitrarily treated, but who is without a union or contract, is generally left with fewer rights in the private sector environment.

Generally, employment actions by private employers do not trigger constitutional protections because the Constitution is designed to curb government excesses. The term used is *State action*, which includes actions by both state and federal governments. If no State action is involved, no constitutional protections are triggered. An employment action by a private employer is considered to be a private action.

Whether there should be a right to privacy in both the public and the private sectors, employers suggest that the employee has three choices when faced with objectionable intrusions by employers: quit, comply, or object and risk termination. Employees argue that they are defenseless because of their economic condition and that their privacy in the private sector is subject to greater abuse precisely because there are no protections and that the option to quit is unrealistic.

One explanation offered for the difference between public- and private-sector privacy protections is compliance-related costs. The implementation of the Privacy Act throughout its agencies costs the government relatively little because it is conducting self-regulation.

By contrast, ensuring compliance within the private sector requires administration of the compliance and adjudication of violations. The Privacy Protection Study Commission found that requiring an employer to change its manner of maintaining and using records can drastically increase the cost of operation.

These costs include the costs of changing employment record-keeping practices, removing relevant information from employment decisions, and implementing a social policy of employee privacy protection. These costs are not necessarily burdensome to the employer, however. One study found that protecting the rights of employees on a computer system could cost as little as $4 per person. Employers' concern for compliance costs may well be an unrealistic barrier to the development of regulations for privacy rights of private-sector employees.

A second distinction between public- and private-sector employers offered to justify different privacy standards is that more stringent regulation is needed for government employees because it is common for federal agencies to be overzealous in surveillance and information gathering. Private-sector employers, in contrast, do not generally have similar resources and, therefore, are unable to duplicate these invasive activities.

Legal Framework for Employee Rights in the Private Sector

Employment-at-will Absent a particular contract or other legal obligation that specifies the length or conditions of employment, all employees are employed "at will." This means that, unless an agreement specifies otherwise, employers are free to fire an employee—and employees are free to leave the position—at any time and for any reason. By virtue of the inherent imbalance of power in the relationship, this mutuality is often only in theory.

LO6

In almost every state,[23] employment is considered to be "at will." **Employment-at-Will** means that the employee serves at the will of the employer. Employers can therefore fire an employee for incompetence, insubordination, or any of the other reasons we might consider valid, as well as because the employee wore red shoelaces to work or because the manager's beloved Lakers lost an important game in double overtime the night before. The point is that employees serve at the whim of the employer. In the same manner, an employee at will may opt to leave a job at any time for any reason, without offering any notice at all; so the freedom is *theoretically* mutual; though, of course, the power balance is not always equal.

Even in at-will states, employees maintain a right to work (see Exhibit 14-4, *"Protecting the Right to Work in the At-Will Employment Context"*). First, as we

Exhibit 14.4 *Protecting the Right to Work in the At-Will Employment Context*

1. Federal and state statutory protections, such as anti-dicrimination laws.
2. Employment contracts, where they exist.
3. Collective bargaining agreements, where applicable.
4. State law exceptions to employment at will, including violations of public policy, breaches of implied contracts, or other statutory exceptions.

have seen in other chapters, federal and state laws protect employees from certain employment actions, such as those based on discrimination against one of the protected classes, including gender or race. Second, an employee who signs an employment contract has those rights stated in the contract. Third, union employees have the protections guaranteed to them by the collectively bargained contract between the employer and the union.

Finally, employment at will is limited by certain exceptions created either by statute or case law. Some states recognize one or more exceptions, while others might recognize none at all. In addition, the definition of these exceptions may vary from state to state.

- Bad faith, malicious or retaliatory termination in violation of *public policy.*
- Termination in breach of the *implied covenant of good faith and fair dealing.*
- Termination in breach of some other *implied contract term*, such as those that might be created by employee handbook provisions (in certain jurisdictions).
- Termination in violation of the doctrine of *promissory estoppel* (where the employee reasonably relied on an employer's promise, to the employee's detriment).
- Other exceptions as determined by *statutes* (such as the Worker Adjustment and Retraining Notification Act [WARN]).

If an employee wishes to recover against an employer in an at-will relationship, the employee must be able to point to a law, court decision, or contractual provision that protects her or him. In the area of privacy, given the absence of any comprehensive national privacy law, that task might be quite difficult.

Bases for Right to Privacy in the Private Sector

Private-sector employers are not bound by constitutional structures. On a state-by-state basis, however, private-sector employees may be afforded protection either by the common law or by statute. All but two states provide common-law tort claims to protect individual privacy, such as intrusion into seclusion. Various torts described below have developed to protect individual solitude, the publication of private information, and publications that present personal information in a false light. (See Exhibit 14.5, "U.S. Companies with Operations in Europe Must Comply with Data Protection Laws," for the manner in which privacy protection is handled somewhat differently in the European context.)

Statutory Claims

State legislatures have responded to the issue of private-sector employee privacy in one of four ways:

1. Enacting legislation mirroring federal law regarding the compilation and dissemination of information.
2. Recognizing a constitutional right to privacy under their state constitutions, as in California, Illinois, and Arizona. For example, California appellate courts have found that employees terminated for refusing to submit to drug

Exhibit 14.5 *U.S. Companies with Operations in Europe Must Comply with Data Protection Laws*

The European Union's approach to data privacy is completely alien to American companies. But, as a recent decision from CNIL (Commission Nationale de l'Informatique et des Libertés, the French Data Protection Authority) makes clear, an American company with operations in Europe that does not learn how to play by European rules runs a serious risk of getting slapped with a hefty fine.

***

[T]he European Union's Directive governing the protection of individuals' personal data and the processing of such data mandates that the member nations adopt laws that cover all "processing" (defined to include even collection and storage) of data about personally-identifiable individuals. The EU Directive includes provisions addressing, among other things, limitations on the use of date [sic], data accuracy, and data destruction requirements. The Directive is not limited to electronic or computerized data, and therefore reaches written, Internet, and even oral communications.

The EU Directive offers a blueprint for data privacy laws across Europe but, in any given situation, the Directive itself is not legally binding. As to each specific data privacy issue arising within Europe, the *relevant country's* local statue [sic] that adopts ("transposes") the Directive will determine data privacy rights an[d] responsibilities.

The Extraterritorial Reach of the EU's Data Privacy Directive Means That *Any* Company with Operations in Europe Must Comply; Cross-Border Data Transfer Is Particularly Thorny

An important aspect of the directive for businesses headquartered outside of Europe, such as in the United States, is the directive's extraterritorial reach. The directive specifically prohibits sending personal data to any country without a "level of [data] protection" considered "adequate" by EU standards. Significantly, the EU has ruled that the United States, with its patchwork of privacy laws, does *not* possess an adequate level of data protection.

The directive authorizes a number of exceptions, legally permitting transmission of personal data outside of Europe even to a "third country" that fails to offer an "adequate level of protection."

Exceptions Permitting Cross-Border Transfers of Personal Data

The EU recognizes three "transborder data flow vehicles": (i) a company can self-certify with the U.S. Department of Commerce that it adheres to specified data protection principles (known as the "safe harbor" system); (ii) a company can enter into "model contracts" with its European subsidiaries, agreeing to abide by mandatory data protection provisions; or (iii) a company can develop a set of "binding corporate rules"—company-drafted data protection regulations that apply throughout the company, which must be ratified by each EU member state's data protection authority. Failure to implement at least one of these methods could result in significant liability.

Obtaining the data subject's free, unambiguous consent to transmit his or her data overseas is theoretically another permissible way in which to transfer data to a country outside the EU—even to a country without comparable data protection law—provided that the consent specifically lists the categories of data and the purposes for the processing outside the EU. Practically speaking, however, obtaining consent to legitimize a transfer overseas is often not an available alternative for employers; in the employment context, because of the imbalance in bargaining power between employer and employee, consents may be presumed *not* to have been freely given.

Also, of course, there is no prohibition against transmitting genuinely *anonymized* data out of the EU. Where the identity of the data subject is impossible to determine, the data transmission falls outside the scope of the directive.

***

Source: Labor & Employment Practice Group, Proskauer Rose LLP © 2008. Reprinted with permission.

tests were wrongfully discharged in violation of the state's constitutional guarantee of a right to privacy, which requires employers to demonstrate a compelling interest in invading an employee's privacy. In Pennsylvania, a court held that a drug test violates that state's policy against invasions of privacy where the methods used do not give due regard to the employee's privacy or if the test results disclose medical information beyond what is necessary. Other states that provide constitutional recognition and protection of privacy rights include Alabama, Florida, Hawaii, Louisiana, Montana, South Carolina, and Washington. However, in all states except California, application of this provision to private-sector organizations is limited, uncertain, or not included at all.

3. Protecting employees only in certain areas of employment, such as personnel records or the use of credit information.
4. Leaving private-sector employees to fend for themselves while the federal laws and the Constitution afford protection to federal employees and those subject to state action.

Tort Law Protections/Common Law

As mentioned above, courts in almost all states have developed case law, the "common law," which identifies certain torts in connection with private-sector invasion of privacy. Georgia was the first jurisdiction whose courts recognized a common-law right to privacy. As the court explained in *Pavesich v. New England Life Ins. Co.*,[24] "a right of privacy is derived from natural law, recognized by municipal law, and its existence can be inferred from expressions used by commentators and writers on the law as well as judges in decided cases. The right of privacy is embraced within the absolute rights of personal security and personal liberty." Though some states rely on statutory protections rather than common law, only two states—North Dakota and Wyoming—fail to recognize *any* of the four privacy torts discussed in this chapter.[25] A **tort** is a legal wrong, for which the law offers a remedy. The torts of particular interest in this chapter include intrusion into solitude or seclusion, the publication of private information, and publication that places another in a false light. Defamation also will be discussed.

tort
A tort is a private (i.e., civil as opposed to criminal) wrong in which one person causes injury to another person, and which allows the injured person to sue the wrongdoer and to collect damages. The injury can be physical, mental, or financial.

Publication as used in these torts means not only publishing the information in a newspaper or other mass media but generally "bringing it to light" or disseminating the information. In addition, the concept of publication is defined slightly differently depending on the tort. Truth and absence of malice are generally not acceptable defenses by an employer sued for invasion of an employee's privacy. They are acceptable, however, in connection with claims of defamation.

LO7

Intrusion into Seclusion The *prima facie* case for the tort of intrusion into seclusion is listed in Exhibit 14.6. (For a more detailed discussion of *prima facie* cases, please see Chapter 3.)

Exhibit 14.6 Prima Facie *Case for the Tort of Intrusion into Seclusion*

To state a *prima facie* case for the tort of intrusion into seclusion, the plaintiff employee must show that

- The defendant employer intentionally intruded into a private area.
- The plaintiff was entitled to privacy in that area.
- The intrusion would be objectionable to a person of reasonable sensitivity.

The intrusion may occur in any number of ways. An employer may

- Verbally request information as a condition of employment.
- Require that its employees provide information in other ways such as through polygraphs, drug tests, or psychological tests.
- Require an annual medical examination.
- Ask others personal information about its employees.
- Go into private places belonging to the employee.

Any of these methods may constitute a wrongful invasion that is objectionable to a reasonable person. On the other hand, if the employer can articulate a justifiable business purpose for the inquiry/invasion, the conduct is may be deemed acceptable.

Rogers v. Loews L'Enfant Plaza Hotel[26] was a case where the intrusion was found to be objectionable. In that case, an employee was continually sexually harassed by her supervisor, including bothersome telephone calls to her home, during which he made lewd comments to her about her personal sex life. The sexual harassment evolved into harassment in the workplace, where the supervisor verbally abused her in front of her co-workers, kept important business-related information from her, and refused to include her in meetings. Her employer, refusing to take formal action, suggested that she change positions. The court determined that the telephone calls were not of a benign nature but, instead, were unreasonably intrusive and not normally expected. Further, the harassment constituted an intrusion into a sphere from which the employee could reasonably exclude the defendant. On these bases, the court found in favor of the employee.

1 Scenario

In connection with *opening scenario 1,* Aravinda's decision in connection with the HIV tests may be governed in part by the law relating to employment testing

Exhibit 14.7 *The* Prima Facie *Case for the Tort of Public Disclosure of Private Facts*

To state a *prima facie* case for the tort of public disclosure of private facts, the plaintiff employee must show that

- There was an intentional or negligent public disclosure
- Of private matters, and
- Such disclosure would be objectionable to a reasonable person of ordinary sensitivities.

as discussed in Chapter 3 and in part by the law relating to disability discrimination as discussed in Chapter 12 (since HIV is considered a disability under the Americans with Disabilities Act). On the other hand, the law relating to intrusion into seclusion also would have application here in terms of disclosure of the test results. If Aravinda discloses the results to anyone or, through her actions, leads someone to a belief about the employee's HIV status, she might be liable under this tort. In addition, it is important to consider that it is highly unlikely that Aravinda has any right to know any employee's HIV status as it is unlikely that the information would be job-related. (Can you imagine what employment position might warrant this type of information? Is HIV status ever considered job-related?)

Public Disclosure of Private Facts The *prima facie* case for the tort of public disclosure of private facts is listed in Exhibit 14.7.

The information disclosed must not already be publicized in any way, nor can it be information the plaintiff has consented to publish. Therefore, in *Pemberton v. Bethlehem Steel Corp.,*[27] publication of an employee's criminal record did not constitute public disclosure of private facts because the criminal record did not contain private facts; it was information that was already accessible by the public.

Case 2

As you shall see, at the end of the chapter, in the *Yoder v. Ingersoll-Rand Company a.k.a. ARO case,* the publication also must be made public, which involves more than mere disclosure to a single third party. The public disclosure must be communication either to the public at large or to so many people that the matter must be regarded as substantially certain to become one of public knowledge or one of knowledge to a particular public whose knowledge of the private facts would be embarrassing to the employee. Therefore, publication to all of the employees in a company may be sufficient, while disclosure to a limited number of supervisors may not.

Several states have enacted legislation codifying this common-law doctrine under the rubric of "breach of confidentiality." Connecticut, for instance, has passed legislation requiring employers to maintain employee medical records separate from other personnel records. Other states have limited an employer's ability to disclose personnel-related information or allowed a cause of action where, through the employer's negligent maintenance of personnel files, inaccurate employee information is communicated to a third party.

Publication in a False Light The *prima facie* case of publication in a false light requires that there was a public disclosure of facts that place the employee in a false light before the public if the false light would be highly offensive to a reasonable person and the person providing the information had knowledge of or recklessly disregarded the falsity or false light of the publication.

Voluntary consent to publication of the information constitutes an absolute bar to a false-light action. This type of tort differs from defamation, where disclosure to even one other person than the employer or employee satisfies the requirements. The tort of publicizing someone in a false light requires that the general public be given a false image of the employee. In a false-light action, the damage for which the employee is compensated is the inability to be left alone, with injury to one's emotions and mental suffering, while defamation compensates the employee for injury to his or her reputation in the public's perception.

Note that any of the above claims may be waived by the employee if the employee also publishes the information or willingly or knowingly permits it to be published. For example, in *Cummings v. Walsh Construction Co.,*[28] the employee complained of public disclosure of embarrassing private facts, consisting of information relating to a sexual relationship in which she was engaged with her supervisor. The court held that, where the employee had informed others of her actions, she waived her right not to have her supervisor disclose the nature of their relationship.

As with defamation, an exception to this waiver exists in the form of compelled self-publication, where an employer provides the employee with a false reason as the basis for termination and the employee is compelled to restate this reason when asked by a future employer the basis of departure from the previous job. Therefore, where the employer intentionally misstates the basis for the discharge, that employer may be subject to liability for libel because it is aware that the employee will be forced to repeat (or "publish") that reason to others.

Breach of Contract An employee also may contest an invasion of privacy by her or his employer on the basis of a breach of contract. The contract may be an actual employment contract, collective bargaining agreement, or one found to exist because of promises in an employment handbook or a policy manual.

Defamation *Libel* refers to defamation in a written document, while *slander* consists of defamation in an oral statement. Either may occur during the course of a reference process. And, while the *prima facie* case of defamation requires a

Exhibit 14.8 *The* Prima Facie *Claim for Defamation*

To state a *prima facie* case for the tort of defamation, the plaintiff employee must show that

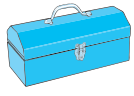
- There were false and defamatory words concerning the employee,
- Negligently or intentionally communicated to a third party without the employee's consent (publication), and
- Resulting harm to the employee defamed.

false statement, even a vague statement that casts doubt on the reputation of an individual by inference can cause difficulties for an employer if it cannot be substantiated.

The elements of a *prima facie* claim for defamation are included in Exhibit 14.8.

One cautious solution to this problem area is to request that all employees fill out an exit interview form that asks, "Do you authorize us to give a reference?" If the applicant answers yes, she or he should be asked to sign a release of liability for the company.

Ordinarily defamation arises from someone other than the defamed employee making defamatory statements about an employee; but one interesting form of defamation has evolved over the past decade where an employee is given a false or defamatory reason for her or his discharge. In that case, the employee is the one who is forced to publicize it to prospective employers when asked for the reason for her or his discharge. These circumstances give rise to a cause of action for defamation, termed *compelled self-disclosure,* because the employee is left with no choice but to tell the prospective employer the defamatory reasons for her or his discharge. Barring this result, the employee would be forced to fabricate reasons different from those given by the former employer and run the risk of being reprimanded or terminated for not telling the truth. This cause of action has been recognized, however, only in Colorado, Iowa, Minnesota, Connecticut, and California. (For a more detailed discussion, see Chapter 3.)



An employer may defend against an employee's claim of defamation by establishing the truth of the information communicated. While truth is a complete defense to defamation, it can be difficult to prove without complex paper management.

Employers also may be immune from liability for certain types of statements because of court-recognized privileges in connection with them. For example, in

some states, an employer is privileged to make statements, even if defamatory, where the statement is made in the course of a judicial proceeding or where the statement is made in good faith by one who has a legitimate business purpose in making the communication (e.g., ex-employer) to one who has a business interest in learning the information (e.g., a prospective employer).[29] This privilege would apply where a former employer offers a good-faith reference to an employee's prospective employer. (See additional discussion of liability for references, below.) "Good faith" means that the employer's statement, though defamatory, is not made with malice or ill will toward the employee.

Regulation of Employee's Off-Work Activities

LO8

Employers may regulate the off-work or otherwise private activities of their employees where they believe that the off-work conduct affects the employee's performance at the workplace. This legal arena is a challenging one since, in the at-will environment, employers can generally impose whatever rules they wish. However, as discussed earlier in this chapter, they may then run afoul of common-law privacy protections. In addition, some states have enacted legislation protecting against discrimination on the basis of various off-work acts. For instance, New York's lifestyle discrimination statute prohibits employment decisions or actions based on four categories of off-duty activity: legal recreational activities, consumption of legal products, political activities, and membership in a union.

Across the nation, there are other less-broad protections of off-work acts. Approximately 30 states have enacted protections specifically on the basis of consumption or use of legal products off the job, such as cigarettes.[30] These statutes originated from the narrower protection for workers who smoked off-duty. Currently, abstention from smoking cannot be a condition of employment in at least 29 states and the District of Columbia (and those states provide antiretaliation provisions for employers who violate the prohibition). In fact, instead of simply identifying the right to use lawful products outside of work, Rhode Island goes further by specifically prohibiting an employer from banning the use of tobacco products while not at work. Some states have responded a bit differently. In Georgia, for instance, certain state workers are charged an additional premium of $40 per month in connection with their state-provided health insurance if they or a covered family member use tobacco products. While the policy is based on an affirmative response to a simple survey question, any employee who misleads the system will lose her or his health coverage for an entire year. The State of Georgia is not alone; a survey by the Society for Human Resource Management found that 5 percent of firms charge a similar premium while 32 percent of firms offer smoking cessation programs as an alternate means by which to reduce costs.

You might be asking yourself, though, how do these firms know? What happens if employees *lie* about their habits? Alaska Airlines uses a preemployment urine screening and will not even hire candidates if they are smokers.[31] For an alternate approach, in what might seem like a program destined for problems, Whirlpool Corporation had imposed a $500 surcharge on employees who

smoked—or at least those who admitted to being smokers—based on its increased benefits costs. When 39 individuals who had not paid the surcharge, thus claiming to be nonsmokers, were observed smoking in the firm's designated smoking areas, they were suspended by Whirlpool for lying. Presumably, they also owed the surcharge.[32]

On the other hand, the issue of weight is handled slightly differently than smoking. Employers are not prohibited from making employment decisions on the basis of weight, as long as they are not in violation of the Americans with Disabilities Act (ADA) when they do so (see Chapter 12). The issue depends on whether the employee's weight is evidence of or due to a disability. If so, the employer will need to explore whether the worker is otherwise qualified for the position, with or without reasonable accommodation, if necessary. If the individual cannot perform the essential functions of the position, the employer is not subject to liability for reaching an adverse employment decision. However, employers should be cautious in this regard since the ADA also protects workers who are not disabled but who are *perceived* as being disabled, a category into which someone might fall based on her or his weight.

One recent trend with regard to weight is to offer incentives to encourage healthy behavior. Some employers have adopted health plans with significantly lower deductibles for individuals who maintain healthier lifestyles (if an employee is not obese or does not smoke, and has yearly physicals). In one audacious statement along these lines, a hospital in Indiana has begun to require its employees to pay as much as $30 every two weeks unless they meet certain company-determined weight, cholesterol, and blood-pressure guidelines.[33]

Laws that protect against discrimination based on marital status exist in just under half of the states. However, though a worker might be protected based on marital *status,* she or he is not necessarily protected against adverse action based on *the identity of the person* to whom she or he is married. For instance, some companies might have an antinepotism policy under which an employer refuses to hire or terminates a worker based on the spouse working at the same firm, or a conflict-of-interest policy under which the employer refuses to hire or terminates a worker whose spouse works at a competing firm.

Because about 40 percent of workers have dated an office colleague, policies and attitudes on workplace dating have the greatest impact.[34] Though only about 9 percent of workplaces have policies prohibiting workplace dating,[35] a New York decision reaffirms the employer's right to terminate a worker on the basis of romantic involvement. In *McCavitt v. Swiss Reinsurance America Corp.,*[36] the court held that an employee's dating relationship with a fellow officer of the corporation was not a "recreational activity" within the meaning of a New York statute that prohibited employment discrimination for engaging in such recreational activities. The employee contended that, even though "[t]he personal relationship between plaintiff and Ms. Butler has had no repercussions whatever for the professional responsibilities or accomplishments of either" and "Swiss Re . . . has no written anti-fraternization or anti-nepotism policy," he was passed over for promotion and then discharged from employment largely because

of his dating. The court agreed with the employer and found that dating was not a recreational activity.

Workplace policies on dating co-workers are largely a function of the employer's corporate culture. Some have banned all inter-office dating, while others permit it. The historical arguments for a ban usually are based on (1) reduced productivity, centered on a belief that such forms of socialization distract the parties involved, (2) potential liability, based on a concern that soured romances may result in harassment charges, or (3) moralistic concerns, particularly in encouraging extramarital affairs. However, to the contrary, some studies suggest that romantically linked employees may be actually more productive, while one study found that couples working in the same location have a divorce rate that is 50 percent lower than the average.[37] The trend today is toward more openness and fewer bans.

The majority of states protect against discrimination on the basis of political involvement, though states vary on the type and extent of protection. Finally, lifestyle discrimination may be unlawful if the imposition of the rule treats one protected group differently from another. For instance, as discussed elsewhere, if an employer imposes a rule restricting the use of peyote in Native American rituals that take place during off-work hours, the rule may be suspect and may subject the employer to liability. Similarly, the rule may be unlawful if it has a disparate impact on a protected group. (For a more detailed discussion of disparate impact and disparate treatment, please see Chapter 3.)

Most statutes or common-law decisions, however, provide for employer defenses for those rules that (a) are reasonably and rationally related to the employment activities of a particular employee, (b) constitute a bona fide occupational requirement, or (c) are necessary to avoid a conflict of interest or the appearance of conflict of interest. For example, drug testing in positions that affect the public safety, such as bus driver, would not constitute an unlawful intrusion because the employer's interest in learning of that information is justified. Where the attempted employer control goes beyond the acceptable realm, courts have upheld an exception to the employment-at-will doctrine based on public policy concerns for personal privacy or, depending on the circumstances, intentional infliction of emotional distress.[38]

2 Scenario

In connection with opening scenario 2, does Abraham have to quit his nighttime dancing job? Recall that Abraham is an at-will employee, making the answer somewhat easier. Since he can be terminated for any reason, as long as it is not a wrongful reason, the partner can impose this condition. But consider Abraham's arguments and the ethical, as well as the legal, implications. As long as Abraham can show that his dancing truly has no impact on his work (i.e., that the club is located in a different town from that of his clientele or that the club has an excellent reputation for beautiful, artistic dancing styles), then he would not have to quit his night job. On the other hand, if Abraham's reputation is soiled by his connection with this club and his boss can show that his work has a negative impact on his ability to perform, then she may be justified in her ultimatum.

In fact, in a case (albeit more extreme) from Arizona, a husband and wife who worked as nurses were fired from a hospital after hospital officials learned that

they ran a pornographic Web site when not at work. The couple explained that they engaged in this endeavor in order to save more money for their children's college education. "We thought we could just do this and it really shouldn't be a big deal," said the husband.[39] Though their dismissal attracted the attention of the American Civil Liberties Union for what it considered was at-will gone awry, the nurses had no recourse. In another case, a police office was docked three days' pay when his wife posted nude pictures of herself on the Internet as a surprise to her husband. However, the pay suspension was justified by the department in that case since police officers could arguably be held to a higher standard of conduct than average citizens.

What about the well-intentioned employer who believes that employees who smoke cigarettes will benefit from a "no smoking any time, anywhere" policy? The employer also may be concerned about the financial impact of disease and other health problems related to smoking. The employer may first encounter obstacles in applying this policy in the workplace itself: Some states specifically prohibit discrimination against smokers in employment. Other states regulate smoking in the workplace only in government agencies or public buildings that are also workplaces. Of course, there are other states, like California, that prohibit smoking in all enclosed places of employment and require employers to warn of any toxic substances in the workplace, including tobacco smoke.[40]

The problem in enforcement would grow as the employer tries to encourage or require employees to quit smoking altogether. How would the employer know whether the employees are smoking when not at the workplace? Would the employer's desire to have healthy employees support the intrusion into employees' decisions regarding their own health? Employers who seek to establish an exercise or "healthy eating" program may encounter similar issues. Emphasizing the work-related benefits of such a program and limiting its reach to the workplace (e.g., creating an exercise room at work where employees may take their breaks if they choose) may allow the employer to reach its goal of a healthier workforce. For more information about this issue, see Exhibit 14.9, "Legal Restrictions on Off-Duty Behavior of Private Employee."

U.S. Companies with Operations in Europe Must Comply with Data Protection Laws

The *City of San Diego v. Roe* case, provided for your review, explores the controversial topic of regulation of private activities away from work. In this case, the employer, the San Diego Police Department, believed that an officer's off-duty activities reflected poorly on the department and were entirely inappropriate. A critical component of the case was the fact that the officer's activities incorporated elements of his duties as a police officer. As you review the case, try to imagine where you would draw the line between appropriate and inappropriate behavior and whether you would have found the employer's actions proper even if no such incorporation of police activities had been involved.

Exhibit 14.9 *Legal Restrictions on Off-Duty Behavior of Private Employee*

Off-Duty Behavior of Private Employee	Business Justification	State Statutory Restrictions on Employer Policy
Illicit drug use	Concern that worker may come to work impaired, jeopardizing the worker's safety and the safety of other workers Quality of work of impaired worker may affect the product or service provided by the company, which, in turn, can affect the business's reputation and profitability Conduct is illegal and not deserving of legal protection	46 states allow employers to test for illicit drugs
Alcohol use	Same justifications as applied to those who use illicit drugs, except for the issue of legality	40 states allow employers to regulate off-duty alcohol consumption
Cigarette smoking	Smokers increase employer's healthcare costs and affect productivity by missing more work due to illness than nonsmokers	22 states allow employers to prohibit off-duty use of tobacco products
Use of weight standards	Same justifications as apply to smokers	49 states allow employers to establish weight standards that do not violate the ADA
Dating between employees	A romantic relationship between employees may affect their productivity The relationship could lead to sexual harassment charges against the employer, especially if one employee is a supervisor of the other Other employees may believe that an involved supervisor is showing favoritism and may then feel that they are victims of discrimination	48 states allow employers to regulate dating between employees
Moonlighting	Working too many hours may impair worker's productivity Working for a competitor could jeopardize privacy of employer information	48 states allow employers to regulate moonlighting
Social relationships with employees of a competitor	Concern that information could be exchanged that would cause harm to the business	48 states allow employers to regulate

Source: Reprinted with permission from John D. Pearce II and Dennis Kuhn, "The Legal Limits of Employees' Off-Duty Privacy Rights," *Organizational Dynamics* 32, no. 4 (2003), pp. 372–83, 376.

Employer's Information-Gathering Process/Justified Use/ Disclosure of Information

The above discussion focused on the scope of the privacy rights of the employee in connection with the dissemination of information. Privacy, however, can be invaded not only by a disclosure of specific types of information but also by the process by which the information has been obtained. An employer may be liable for its *process* of information gathering, storing, or utilization. Improper gathering of information may constitute an invasion where the process of collection constitutes harassment, where improper filing or dissemination of the information collected may leave the employer liable for defamation actions, and/or where inappropriate use of data for purposes other than those for which the information was collected may inflict other harms.

A final concern is called *function creep* and may begin with the voluntary transmission of information by an individual for one purpose for which the individual consents. For instance, an individual may offer personal information to her or his employer without understanding or intending that the employer then share more information than required with the Immigration and Naturalization Service. Similarly, information gathered during a preemployment physical for purposes of appropriate job placement may seem perfectly appropriate to share with an employer; but, the employee might have concerns if that information is later shared with her or his manager or co-workers for other purposes.

The collection or retrieval of information may occur in a variety of ways, depending on the stage of employment and the needs of the employer. For example, an employer may merely make use of the information provided by an applicant on her or his application form, or it may telephone prior employers to verify the data provided by the applicant. One employer may feel confident in an employee's educational background when she sees the employee's diplomas hung on the office wall, while a different employer may feel the need to contact prior educational institutions to verify attendance and actual graduation. On the more lenient end of the spectrum, the employer may rest assured that the employee is all that he states that he is on the application form, while, in more extreme situations, an employer may subject its employees to polygraph analyses and drug tests.

As is covered extensively in other chapters, employers are limited in the questions that may be asked of a potential employee. For example, an employer may not ask an applicant whether she or he is married or plans to have children, or the nature of her or his family's origin. These questions are likely to violate Title VII of the Civil Rights Act; in most cases this is not because the employer should not have the information, literally, but instead because an employer is prohibited from reaching any employment decision on the basis of their answers. In addition, employers are limited in their collection of information through various forms of testing, such as polygraphs or medical tests. These are discussed further in Chapter 3, but employers are constrained by a business necessity and relatedness standard or, in the case of polygraphs, by a requirement of reasonable suspicion. With regard to medical information specifically, employer's decisions are not only governed by the Americans with Disabilities Act

but also restricted by the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191). HIPAA stipulates that employers cannot use "protected health information" in making employment decisions without prior consent. Protected health information includes all medical records or other individually identifiable health information. (See Exhibit 14.10 "Protecting Workers' Personal Data.")

Exhibit 14.10 *Protecting Workers' Personal Data*

In 1997, the International Labour Organization published a Code of Practice on the Protection of Workers' Personal Data. Though not binding on employers, it serves to help codify ethical standards in connection with the collection and use of employee personal information and is recognized as the standard among privacy advocates.[41] The code includes, among others, the following principles:

5. GENERAL PRINCIPLES

5.1 Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.

5.2 Personal data should, in principle, be used only for the purposes for which they were originally collected. . . .

5.4 Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behavior of workers.

5.5 Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.

5.6 Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance. . . .

5.8 Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights. . . .

5.10 The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation. . . .

5.13 Workers may not waive their privacy rights.

6. COLLECTION OF PERSONAL DATA

6.1 All personal data should, in principle, be obtained from the individual worker.

6.2 If it is necessary to collect personal data from third parties, the worker should be informed in advance, and give explicit consent. The employer should indicate the purposes of the processing, the sources and means the employer intends to use, as well as the type of data to be gathered, and the consequences, if any, of refusing consent. . . .

6.5 An employer should not collect personal data concerning a worker's sex life; political, religious, or other beliefs; or criminal convictions. In exceptional circumstances, an employer may collect personal data concerning those in named areas above if the data are directly relevant to an employment decision and in conformity with national legislation.

6.6 Employers should not collect personal data concerning the worker's membership in a workers' organization or the worker's trade union activities, unless obliged or allowed to do so by law or a collective agreement.

6.7 Medical personal data should not be collected except in conformity with national legislation, medical confidentiality and the general principles of occupational health and safety, and only as needed to determine whether the worker is fit for a particular employment; to fulfill the requirements of occupational health and safety; and to determine entitlement to, and to grant, social benefits. . . .

continued

6.10 Polygraphs, truth-verification equipment or any other similar testing procedure should not be used.

6.11 Personality tests or similar testing procedures should be consistent with the provisions of this code, provided that the worker may object to the testing.

6.12 Genetic screening should be prohibited or limited to cases explicitly authorized by national legislation.

6.13 Drug testing should be undertaken only in conformity with national law and practice or international standards.

11. INDIVIDUAL RIGHTS

11.1 Workers should have the right to be regularly notified of the personal data held about them and the processing of that personal data.

11.2 Workers should have access to all their personal data, irrespective of whether the personal data are processed by automated systems or are kept in a particular manual file regarding the individual worker or in any other file which includes workers' personal data.

11.3 The workers' right to know about the processing of their personal data should include the right to examine and obtain a copy of any records to the extent that the data contained in the record includes that worker's personal data. . . .

11.9 Workers should have the right to demand that incorrect or incomplete personal data, and personal data processed inconsistently with the provisions of this code, be deleted or rectified. . . .

11.11 If the employer refuses to correct the personal data, the worker should be entitled to place a statement on or with the record setting out the reasons for that worker's disagreement. Any subsequent use of the personal data should include the information that the personal data are disputed and the worker's statement.

In connection with the storage of the information collected, employers must be careful to ensure that the information is stored in such a manner that it will not fall into the wrong hands. If an improper party has access to the personal information, the employer, again, may be subject to a defamation action by the employee based on the wrongful invasion of her personal affairs, as discussed above. In today's world of advanced computer data storage, new issues arise that have not been previously litigated. For instance, where an item is stored in a computer, it is crucial either to close the file to all but those who have a correct entry code or to delete private information. Access to computer terminals throughout an office creates a problem concerning the dissemination of the private information and the control of access.

The employer offering the reference is responsible for its dissemination only to appropriate parties. A fax machine or postcard would be unacceptable means of transmitting a reference since this would allow access by innumerable others. Similarly, an employer may get caught wrongfully disclosing information to an inappropriate individual in the case of the telephone reference. Failure to confirm the identity of the caller and purpose of the call may allow disclosure to one who otherwise should have no access to this information.

Electronic Monitoring or Surveillance of Employee Activities

With the dramatic increase in the use of technology in the workplace, several issues have recently developed surrounding the use of e-mail and the Internet. Many state and district courts have dealt with the issues differently or have not faced them at all. On the other hand, 84 percent of companies surveyed for a 2007 report have written policies concerning e-mail use, 66 percent engage in some form of e-mail monitoring, and 28 percent have terminated employees for inappropriate e-mail use.[42]

Though, at first blush, blogs might seem an innocent environment in which employees can vent comments regarding their employment situation, imagine the impact of a viral message when placed on the Web and then allowed to have the exponential impact experienced by some blogs. Since it is estimated that blog readership is in the millions,[43] corporate reputations are at stake and legal consequences can be severe; 14 percent of U.S. publicly traded companies investigated a leak of material financial information via a blog in the past 12 months.[44] In one situation, a Google employee compared the firm's health plan to Microsoft's, and it did not fare too well. He also blogged about how the company's provision of free food was merely an incentive to work through the dinner hour. The employee was subsequently terminated. The term to be "dooced" refers to having lost one's job as a result of one's Web site.[45] Consider the challenges involved in the implementation of a companywide blogging policy, as discussed in Exhibit 14.11, "Bloggers Beware: New Rules for CBC Employees." For more on blogging and social media generally, see below.

Exhibit 14.11 *Bloggers Beware: New Rules for CBC Employees*

My name is Chris MacDonald, and I work for the Canadian Broadcasting Corporation. OK, that second part isn't true, but if it were, I might not be allowed to write this blog, or at least I wouldn't be allowed to tell you who I work for, according to a new "guideline" issued by the CBC's management. (CBC managers have asserted that it's a guideline, not a policy. As far as most of the concerns about the document are concerned, it's a spurious distinction.)

The document is not publicly available—in fact, it hasn't been officially distributed within the CBC yet—but it got leaked internally, and lots of CBC employees have seen it. It caught CBC-based bloggers off-guard; despite the fact that several of them had proactively written their own set of voluntary guidelines a few years ago, they weren't included or consulted in the process of devising the new official guideline.

According to the InsideCBC blog (an official, sanctioned, insider's blog), the new policy applies to a CBC employee's personal blog "if the content clearly associates them with CBC/Radio-Canada."

Among the requirements of the guideline/policy:

- Bloggers are "expected to behave in a way that is consistent with our journalistic philosophy, editorial values and corporate policies."
- "[T]he blog cannot advocate for a group or a cause, or express partisan political opinion. It should also avoid controversial subjects or contain material that could bring CBC/Radio-Canada into disrepute."
- To start and maintain a blog of this kind, you need your supervisor's approval.

continued

Note, also, that the guideline/policy applies to *all* employees, not just to journalists (whose blogs might reasonably be mistaken for news) or to marquee on-air personalities.

The guideline has caused a stir among CBC-employee-bloggers and beyond.

A lot of objections have already been raised in the Comments section of the InsideCBC blog. And while some elements of the document seem unproblematic and even constructive, I see a couple of *types* of problems with it. One has to do with content. The other has to do with process.

Content:

There are clearly a number of elements of the guideline/policy that are either unclear or unenforceable or both. For example, the stipulation that it applies to blogs "if the content clearly associates them with CBC/Radio-Canada." Several commentators have pointed out that there are lots of ways, intentional and unintentional, that a blog could associate itself with the CBC. The blogger might self-identify as a CBC employee, or merely imply or even just let slip that she or he is an employee. In terms of specific requirements, the one that has most angered those involved is the stipulation that employees must seek their supervisors' *permission* to write a *personal* blog. This seems on the face of it a pretty serious restriction on freedom of speech. Maybe (maybe) CBC has the right to make that stipulation as a matter of employment contract, but having a right to do so doesn't make it appropriate, or wise, to exercise that right.

Process:

It's pretty bad that bloggers at the CBC were caught off-guard by this guideline/policy, for at least 3 reasons

1) For policies and codes of all kinds, buy-in is crucial. Given how difficult this policy will be to enforce (i.e., very) it's utterly essential that the people to be governed by it accept it as legitimate and wise. Oops.
2) The CBC employees with blogs are a pretty smart bunch, who have thought a fair bit about what their obligations are. And, just through experience, they understand blogging better than anyone in CBC's editorial offices is going to. What a shame not to draw on that knowledge and experience. Serious error.
3) By drafting a document that doesn't reflect, acknowledge, or draw upon the bloggers' own manifesto, CBC management is neglecting the fact that some of their very bright employees have expected considerable effort on the very issue they're now seeking to regulate. At the very least, that seems disrespectful.

Now that the errors have been made, the serious ethics & leadership challenge lies in whether & how CBC managers can recover. "Recovery" here means ending up with a policy that is clear and enforceable, and retaining some semblance of moral authority in the eyes of their employees.

Disclosure of potential bias: I've got a friend among the CBC-employee-bloggers affected by this new guideline/policy.

Update

According to [an] update, the document referred to above was "only a proposed early draft." (Note that "proposed" doesn't make sense there: either it was a draft, or it wasn't.) Also according to the update, "There are currently no specific corporate policies in effect relating directly to blogging." (This update is brought to you by the nice Media Relations and Issues Management people at CBC, who asked me to correct the above posting.)

Source: Christopher MacDonald, "Bloggers Beware: New Rules for CBC Employees," August 6, 2007, http://www.businessethics.ca/blog/2007/08/bloggers-beware-new-rules-for-cbc.html. © Christopher MacDonald, reprinted with permission.

Author's note: The blog that includes the text of the CBC update mentioned above also includes the original text of the introduction to the blogging policy that indicates nowhere that the document contained "proposed" guidelines. Instead, it said, "[a]ttached are personal blogging guidelines the Editor in Chief's office distributed a while back."

Exhibit 14.12 *Implications of New Technology*

Consider the implications of new technology on the following areas:

- Monitoring usage.
- Managing employee and employer expectations.
- Distinguishing between work use and personal use of technology.
- Managing flextime.
- Maintaining a virtual workplace.
- Protecting against medical concerns for telecommuters.
- Managing/balancing privacy interests.
- Monitoring die use of the Web to spread information and misinformation.
- Managing fair use/disclosure.
- Responding to accessibility issues related to the digital divide.
- Managing temporary workforces.
- Adapting to stress and changing systems.
- Maintaining proprietary information.
- Measuring performance.
- Managing liability issues.

LO9

Of course, little did anyone anticipate what dilemmas would arise as a result of advances in technology over the past few decades. Who would have thought that one might begin her or his workday by placing a hand on a scanner to confirm one's identity and time of arrival at work[46] or that location-based technologies would allow employers to know an employee's whereabouts at all times?[47] Notwithstanding issues in connection with production, marketing, finance, and other areas of a firm's operations, we now have countless issues that intersect law and ethics with which we were never before confronted. (See Exhibit 14.12.)

Where technology will take employer monitoring is anybody's guess; but a few recent trends may point the way. Global positioning systems (GPS) are now ubiquitous, but employer use has so far been mostly confined to vehicle tracking such as on over-the-road trucks. Look for GPS to spread to employee tracking, for example, by including such devices in nametags, uniforms, key chains, or other devices that employees may carry.

A related technology is called radio frequency identification devices (RFID), which are microchips that can be planted anywhere, including under the skin. In 2006, Citywatcher.com became the first U.S. firm to ask employees to accept RFID bodily implants.[48] Those who refused the implant were required to carry a keychain with an RFID microchip. While one's first instinct might be a concern about privacy, consider the reasoning used by the attorney general in Mexico who explained why he opted to implant the tiny devices under the skin of some of his workers. He sought to justify the use of the devices in order to track them more effectively in case they were kidnapped because of their line of work. Companies uncomfortable with implementation are considering alternatives such as imbedding the microchips in clothing or employee IDs.

States are concerned enough about the possibility of the widespread use of RFID implants that they have begun to act. In 2006, Wisconsin became the first

state to ban mandatory implants.[49] North Dakota, California, and Missouri have since followed course, with other states considering similar legislation.

Biometrics is an identification technology that includes fingerprints, voice recognition, and iris recognition. Proposals for a national identification card incorporate biometric technology in order to establish an individual's identity. Biometric Social Security cards and biometric employment cards have also been proposed.[50] Some employers see biometrics as a more modern version of the time clock, while employees tend to view it more ominously. It seems inevitable that most employers will ultimately incorporate some form of biometric technology into their employee-monitoring arsenal.

Though seemingly monumental on the surface, advances in the information-gathering abilities of these technologies are actually merely geometric rather than exponential. Employers have always gathered information about their employees; the only element that has changed in recent decades is how that information is collected rather than the values that underlay the decision to do so.

For instance, Milton Hershey of Hershey's Chocolate used to tour Hershey, Pennsylvania, to see how well his employees maintained their homes. He hired detectives to spy on Hershey Park dwellers in order to learn who threw trash on its lawns. Henry Ford used to condition wages on his workers' good behavior *outside the factory,* maintaining a Sociological Department of 150 inspectors to keep tabs on workers. Technology, therefore, does not present us with new value judgments but, instead, simply presents new ways to gather the information on which to base them. Sorting through these issues is challenging nevertheless. Consider the impact of September 11, 2001, on an employer's decision to share personal employee information with law enforcement. Private firms may be more willing today to share private information than they would have been previously. Consider more specifically the issues raised above and the implications of technology on some of these traditional workplace challenges:

- Technology allows for in-home offices, raising issues of safety as well as privacy concerns; there are now more than 33.7 million U.S. telecommuters.[51] (Efforts by OSHA in the late 1990s to impose workplace safety standards on home offices received huge flack!)
- Technology allows for greater invasions by the employer but also allows for additional misdeeds by employees.
- Technology blurs the lines between personal and professional lives.
- Technology allows employers to ask more of each employee—each is capable of much greater production.
- What constitutes a "workday"? When is enough enough?
- Should the ability to find something out make it relevant (e.g., off-work activities)?
- Many of the new technologies (e-mail, voice mail) allow for faceless communication.

- Research has shown that excessive exertion of power and authority over employees may actually lead to insecurity, feelings of being overwhelmed and powerless, and doubts about worthiness.[52]

"The psychological impact of constant observation is serious and represents a major assault on the ethical rights of workers. Furthermore, productivity may also be compromised as a by-product of the growth of surveillance in the workplace."[53]

Consider the following overview of the implications of the technology economy as reported in the *World Employment Report 2001,* issued by the International Labour Office:

> More and more, boundaries are dissolving between leisure and working time, the place of work and place of residence, learning and working. . . . Wherever categories such as working time, working location, performance at work and jobs become blurred, the result is the deterioration of the foundations of our edifice of agreements, norms, rules, laws, organizational forms, structures and institutions, all of which have a stronger influence on our behavioral patterns and systems of values than we are aware.[54]

Finally, intrusions may come from unexpected arenas. For instance, while employees perhaps are concerned about their rights with regard to employer monitoring in the workplace, they might contemplate the possibility of informal intrusions such as from their colleagues rather than their supervisors. In a 2007 survey of information technology employees, a security vendor found that one-third of 200 respondents admitted to having used their administrative passwords in order to access confidential employee information including compensation information. One of the survey respondents was quoted as saying, "Why does it surprise you that so many of us snoop around your files? Wouldn't you if you had secret access to anything you can get your hands on?"[55] Unfortunately, this same survey reported that access continued long after many of these respondents had left their employers. Further exploration into the subject only uncovers greater vulnerabilities. In a much larger survey of more than 16,000 IT practitioners, almost two-thirds reported that they had intruded into another employee's personal computer without permission, and this number includes one-third of respondents who were at the manager level or above!

Forms of Monitoring

Monitoring in the workplace can take several forms and occurs for numerous reasons. Privacy scholar Colin Bennett identifies four types of surveillance that can specifically impact workers.[56] The first is *surveillance by glitch,* in which information is uncovered by mistake. This occurred, for example, when Microsoft discovered that expired Hotmail accounts retained buddy lists, which were then shared with new subscribers who were given those accounts' e-mail addresses. In the workplace, a glitch could occur when a technician checks to see if a computer's hard drive has been erased by the previous user for use by someone else. That technician might notice inappropriate content on the hard drive. A similar circumstance

arose when the dean of Harvard's Divinity School asked a Harvard information management technician to do some work on his Harvard-owned laptop. The technician found inappropriate pornographic materials, and the media frenzy that erupted has only recently subsided. Oddly enough, the CFO of Mesa Airlines *defended* himself with pornography in a different case where he was accused of deleting company information to an ongoing lawsuit from three computers. Instead, he claimed, he was simply trying to delete files of pornography he had downloaded and that he thought might embarrass him. Funny how our concepts of the "lesser evil" shift, depending on the nature of the harm done.[57]

In another example of a glitch or mistake, cheating by a worker in a government agency was discovered when the worker left a copy of a stolen promotion exam in the copying machine. Such glitches may uncover violations of a usage policy even when no systematic monitoring is being conducted.

Bennett's second form of surveillance is *surveillance by default.* This occurs when the default setting is "monitor," whereby all information that is sent through a system is caught and cataloged. An example of this type of monitoring would be the "Cue Cat." A Cue Cat is a mouse-like device that was sent to subscribers of certain magazines. They were told that they could scan bar codes in the magazine in order to gather more information on the accompanying topics later through their computers. What these users were not told was that each Cue Cat was individually coded to send subscriber information along with the information request. Therefore, the publishers or advertisers were able to surreptitiously collect data from anyone who used the device at all times. In the workplace, surveillance by default occurs when there is a video camera recording every transaction or activity by default, rather than recording only specific activities. Though they did not repeat the question on subsequent surveys, the American Management Association reports that 75 percent of firms surveyed in 2001 regularly record their employees' e-mail transmissions by means of a default setting.[58]

The third form of monitoring is *surveillance by design,* where the entire purpose of the technology is to collect information and, generally, the user is aware of this purpose. Supermarkets often trade discounts on products in exchange for an individual's personal information on the application form for the encoded key chain device that allows the discount. The shopper is fully aware of the exchange when the information is collected, and the entire purpose of the key chain device is to provide information to the store. Often customer service representatives will be notified by an audible "beep" on the telephone that they are being monitored, and they understand that this monitoring will have implications for their performance evaluations. Another type of surveillance by design occurs when firms conduct either random or periodic keyword searches of e-mail or other transmissions. One-fourth of firms surveyed by the American Management Association reported that they perform keyword searches, generally seeking sexual or scatological language to protect themselves from later liability.[59]

Surveillance by possession exists where the employer maintains employee information in a database or some other list. Bennett refers to this form of surveillance

as gathering information that could be sold or acquired, such as employee personal information from application forms.

Much of the monitoring that occurs today in American firms is surveillance by design or by default. For instance, an e-mail program that systematically sorts and saves all e-mail that contains certain terms (such as those used in a job search or those that might be considered sexually harassing) would constitute surveillance by default. A monitoring program that tracks Internet accesses and blocks inappropriate Web sites would be surveillance by design.

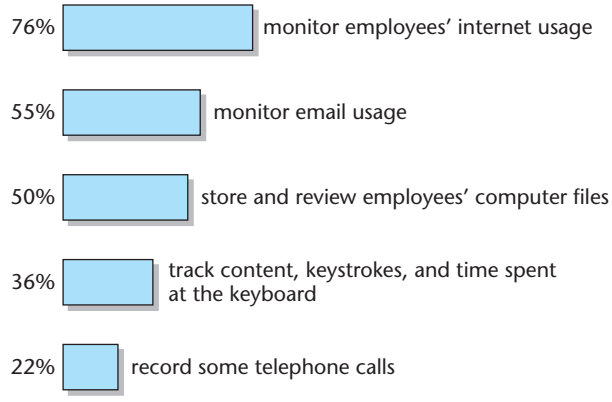
How Does Monitoring Work?

Advances in information-gathering technology have allowed monitoring to an extent that was never before possible. Worldwide sales of monitoring technology are estimated at $140 million annually.[60] One example of this new technology is Raytheon's Silentrunner, which allows firms to track everything that occurs on a network, including not only e-mail but also instant messaging ("IM," one of the ways employees thought they had foiled e-mail monitoring).[61] Approximately 11 million people in the United States use IM at work.[62] While some firms may encourage its use since it can cut down on travel, in-person meeting, and conference call expenses, IM also poses a significant risk since there is no built-in security measure in IM systems.

Other products called location-based monitoring services allow trucking firms to track their vehicles across the nation using global positioning[63] or allow managers to test a worker's honesty by using a truth-telling monitor during telephone calls.[64] The most prevalent Internet-monitoring product in the United States is Websense, with 8.25 million users worldwide. While Websense merely *blocks* certain Web sites, Websense Reporter, an add-on, records all Web accesses—not only attempted accesses blocked by Websense but also all nonprohibited Web surfing (70 percent of Websense's customers install Reporter). MIMEsweeper is the most used e-mail monitoring system in the United States, with 6,000 corporate customers and over 6 million ultimate users worldwide. In a less-publicized form of monitoring, SWS Security offers a product that allows managers to track the messages a worker receives on a portable paging device so that one could track whether the employee is being distracted by outside messages. Another provider, www.tracingamerica.com, offers the following information at the listed prices:

- Social Security numbers, $25.
- General all-around background search, $39.
- Countywide search for misdemeanors and felonies, $35.
- Whether subject has ever spent time in prison, $25.
- Whether subject has ever served time in a federal prison, $50.
- National search for outstanding warrants for subject, $50.
- Countywide search for any civil filings filed by or against subject, $50.
- Subject's driving record for at least three years back, $30.

Exhibit 14.13 *Percentage of Large U.S. Companies That Monitor Technology Usage*



Source: Adapted by authors from data from the American Management Association, "2007 Electronic Monitoring & Surveillance Survey," March 13, 2008, www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx.

In the American Management Association's 2007 survey,[65] 43 percent of the respondents reported that they engaged in e-mail monitoring as a result of their concerns for legal liability (Exhibit 14.13, "Percentage of Large U.S. Companies That Monitor Employee E-mail"). Monitoring does not stop with e-mail and the Internet; the ACLU reports that employers monitor an estimated 400 million telephone calls annually.[66] Given the courts' focus in many cases on employer response to claims of sexual harassment or unethical behavior, among other complaints, firms believe that they need a way to uncover these inappropriate activities. More than 24 percent of firms have reported receiving a subpoena for employee e-mail, and 26 percent of the firms reported firing employees for inappropriate e-mail.[67] Without monitoring, how would companies know what occurs? Moreover, as courts maintain the standard in many cases of whether the employer "knew or should have known" of wrongdoing, the state-of-the-art definition of "should have known" becomes all the more vital. If most firms use monitoring technology to uncover such wrongdoing, the definition of "should have known" will begin to include an expectation of monitoring. Finally, some recent state cases have held that, where an employer provides notice to employees that e-mail is the property of the employer and that it will be monitored, communications by the employee over that system cannot be privileged or confidential, *even if sent to a private attorney.*[68]

One of the most recent advances in monitoring technology involves the use of biometrics, including identification by fingerprint verification, iris and retinal scanning, hand geometry analysis, or facial feature scanning. Approximately 6 percent of employers in the United States use biometrics for a variety of purposes from

allowing customers to purchase goods and services or for airline check-in. Those in favor of the technology contend that it will reduce the high economic and emotional costs of identity theft, among other benefits. Those opposed argue that it is subject to inaccuracies, provides more information than employers have a right to know, and is one additional way in which "big brother" can keep an eye on employees at all times.

Employee theft has led both public and private employers to increase monitoring of their employees by using video surveillance. According to the National Retail Security Survey, 47 percent of an annual retail loss to employers of almost $37.4 billion in 2005 was due to employee theft—more than $17 billion.[69] Another study conducted in 2005 by Hayes International reported that one out of every 26.5 employees was apprehended for theft from her or his employer in 2005. The survey also found that respondents caught 68,994 dishonest employees in 2005, which represented an increase of 11.49 percent over 2004's apprehensions, and that money gained by identifying dishonest employees totaled over $49.9 million.[70] Nevertheless, video surveillance may cost the employer through loss of morale. "Would you like to work in an environment where every time you blow your nose . . . it's on videotape?" asks Lewis Maltby, president of the National Workrights Institute in Princeton, New Jersey.[71]

While no case of employer monitoring has yet reached the Supreme Court, these actions have received lower-court attention. As early as 1990, Epson America survived a lawsuit filed by a terminated employee who had complained about Epson's practice of reading all employee e-mail.[72] In that case, the court distinguished the practice of *intercepting* an e-mail transmission from storing and reading e-mail transmissions once they had been sent. However, relying on court precedent for protection is a double-edged sword. An employee-plaintiff in one federal action won a case against his employer where the employer had monitored the worker's telephone for a period of 24 hours in order to determine whether the worker was planning a robbery. The court held that the company had gone too far and had insufficient evidence to support its claims.[73] In another action, Northern Telecom settled a claim brought by employees who were allegedly secretly monitored over a 13-year period. In this case, Telecom agreed to pay $50,000 to individual plaintiffs and $125,000 for attorney fees.[74]

Courts have supported reasonable monitoring of employees in open areas as a method of preventing and addressing employee theft. For example, in *Sacramento County Deputy Sheriff's Association v. County of Sacramento,*[75] a public employer placed a silent video camera in the ceiling overlooking the release office countertop in response to theft of inmate money. The California Court of Appeals determined that the county had engaged in reasonable monitoring because employee privacy expectations were diminished in the jail setting.[76]

Though courts do not, per se, *require* notice in order to find that no reasonable expectation of privacy exists and to therefore allow monitoring by employers, notice of monitoring is favored by the courts.[77] The court in *Thygeson v. U.S. Bancorp*[78] held that an employer's specific computer usage policy precluded an employee's reasonable expectation of privacy.

While, as stated earlier, there is little legislation that actually relates to these areas specifically, there is some statutory protection from overt intrusions, though the statute does not apply in all circumstances. The federal wiretapping statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986,[79] protects private- and public-sector employees from employer monitoring of their telephone calls and other communications without a court order.

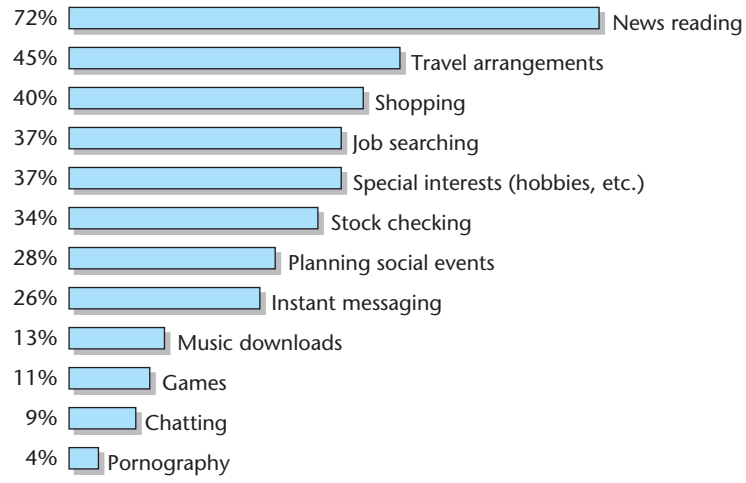
There are two exceptions to this general prohibition. First, interception is authorized where one of the parties to the communication has given prior consent. Second, the "business extension" provision creates an exception where the equipment used is what is used in the ordinary course of business. An employer must be able to state a legitimate business purpose and there must be minimal intrusions into employee privacy such that they would not be objectionable to a reasonable person.

The employer's right to monitor private communications from an employee is not absolute, regardless of what the company policy might say.[80] Limits do exist. For example, in *Stengart v. Loving Care Agency, Inc.,*[81] the New Jersey Supreme Court ruled that communications between an employee and her attorney, which involved potential employment discrimination claims by the employee against the employer, were not subject to monitoring by the employer. Monitoring of those password-protected communications violated both the employee's right of privacy and the attorney-client privilege.

Similarly, in *Pietrylo v. Hillstone Restaurant Group,*[82] a federal court jury found in favor of employees who sued their managers for improperly accessing a password-protected MySpace page that contained criticisms of the managers without the employees' permission. The general rule that can be gleaned from these cases is that employers need permission from the employee to retrieve communications in password-protected areas. The approach taken by the city of Bozeman, Montana, is to require that all prospective employees disclose their user names and passwords for any profiles they have on Facebook, MySpace, Yahoo, Google and YouTube. [83] Whether that approach will hold up in court will have to wait for another day. However, in at least one case, a federal court required that an employee make available to an employer during a trial her complete Facebook and MySpace profiles, even though she had set various information to "private" using the online settings.[84] An interesting question arises as to the extent of an employer's responsibilities once it begins monitoring. If an employee's communications harm some third party, can the third party hold the employer legally responsible for failing to properly monitor the employee? The New Jersey Appellate Division said yes, because employers who tell employees that they will monitor communications have an affirmative duty to monitor and can be liable to a third party for failing to discover the improper behavior.

For example, in *Doe v. XYZ Corporation,*[85] the employee was visiting a pornographic Web site while at work. His manager knew about this activity, but never mentioned it to the IT department. It turned out that the Web site involved not just child pornography, but the employee's own stepdaughter. The stepdaughter was allowed to pursue a claim against the employer for failing to properly monitor the employee's online activities.

Exhibit 14.14 *Surfing on the Job: Most Popular Nonwork-Related Internet Usage.*



Source: Adapted by authors from data from the American Management Association, "2007 Electronic Monitoring & Surveillance Survey," March 13, 2008, www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx.

Business Justifications for Monitoring Employees' Technology Use

LO10

Web access at work may allow employees to be more creative and productive, but it also creates great risks. A survey by the Web site Vault.com found that 90 percent of employees surf non-work-related Web sites while at work.[86] (See Exhibit 14.14, "Surfing on the Job: Most Popular Nonwork-Related Internet Usage.") Wasted time, overclogged networks, and inappropriate material seeping into the workplace are all reasons why employers may seek to limit employees' Internet use at work. Of employers who monitor, almost half report that they restrict employees' Internet use.[87]

3 Scenario

As mentioned above, monitoring is made simpler through an employee's use of a computer. Employers now customarily provide many employees with personal computers that are linked either to the Internet or, at least, to an internal network. Employers can monitor the computer user's activities. As to the type of information that can be gathered, the Privacy Demonstration Page of the Center for Democracy and Technology can feed back to viewers information that it finds out merely because one has accessed the page. For instance, the page tells one individual viewer the type of computer that the viewer is using, the browser the individual is using, the server from which the viewer is operating, and some of the pages the viewer has recently visited. While this information may not necessarily seem personal to some, consider the facts of scenario two. The employer in that case seems to be within its rights to monitor the use of its computers.

The need to monitor employees' usage becomes clear when one focuses on five areas of potential employer liability: defamation, copyright infringement, sexual harassment, discrimination, and obscenity.

As discussed previously in this chapter, the guidelines that apply to a general defamation claim also apply to issues surrounding the Internet. However, some contend that the opportunity for harm is far greater. This is because employees and employers can easily disseminate information to a wide range of media. Not only can employers be subject to defamation claims by their own employees, but the far greater threat is the liability a company faces when an employee, as a representative of the employer, defames another individual using the Internet (with access provided by the employer) as the medium.

Further, firms are concerned about inappropriate use of Web software such as occurs when an employee downloads program files without compensating the creator or when employees use copyrighted information from the Web without giving credit to the original author, thereby exposing the firm to potentially significant copyright infringement liability. Finally, when an employee downloads software programs from the Web, the computer systems within the firm have the potential to be compromised by viruses or even unauthorized access.

Sexual harassment and discrimination by employees via the Web are governed by the same general guidelines that were previously discussed in the chapters addressing sexual harassment and discrimination. However, many employees believe that once an e-mail message is deleted, it is permanently removed from the system. This is not the case. Because of this, e-mail sent on company time, with contents that constitute sexual harassment, that might create a hostile working environment, or that contain other forms of discrimination, may easily be discovered, both by the employer and by opposing parties to litigation against the employer. In fact, in one survey, 24 percent of companies had been ordered by a court to produce employee e-mail in the past 12 months.[88] For example, female warehouse employees alleged that a hostile work environment was created in part by inappropriate e-mail, and they sought $60 million in damages in federal court. The case settled out of court.[89] In another case, *Zubulake v. UBS Warburg,* the plaintiff was awarded a jury verdict in the amount of $29.2 million.[90] The award ended up so large in part due to sanctions imposed by the trial judge as a result of the employer's failure to preserve e-mails for evidentiary purposes. E-mail is discussed in greater detail in the next section. Finally, obscenity becomes a critical issue, and the company may be placed at risk when employees download pornographic images while at the workplace.

Moreover, a firm might be concerned about the impression created when an employee visits various sites. Consider these scenarios: A customer service representative at an electronics store is surfing the Internet using one of the display computers. She accesses a Web site that shows graphic images of a crime scene. A customer in the store who notices the images is offended. Another customer service representative is behind the counter, using the store's computer to access a pornographic site, and starts to laugh. A customer asks him why he is laughing. He turns the computer screen around to show her the images that are causing him amusement.

Certainly, the employer would be justified in blocking employees' access to such Web sites. But what about sites of activist groups regarding sensitive issues such as abortion? Should an employer be allowed to block or restrict access to such sites? If such access may be restricted in order to promote efficiency and professionalism, then should employers be allowed to limit access to such innocuous sites as eBay or ESPN.com? The Vault.com survey mentioned above revealed that over half of the employees who make personal use of the Internet at work restrict their surfing to less than half an hour a day. By limiting or restricting access to Web sites, the employer may be creating an environment in which employees do not feel trusted and perhaps feel inhibited about using the Internet for creative, work-related purposes because they fear being reprimanded for misusing access.[91]

Employers seem to have business justification for other types of monitoring: "If [the employer] sees you doing something on the screen that they think you can do in a quicker way, they can tell you. They can even tell you ways to talk to people, or they can tell you ways to do things quicker to end your [customer service] call quicker," says Kathy Joynes, a travel agent for American Express who works out of her home, but whose supervisor can shadow her computer screen at any time.[92]

Because of the overall potential liability for their employees' actions, employers should develop a formal policy or program regulating employee usage of the Internet. In addition to having a formal policy, employers may choose to establish a process of monitoring their employee's Internet usage. This may involve tracking Web sites visited and the amount of time spent at each site using software programs designed for that specific purpose. However, employers need to consider the employees' rights to free speech and privacy when developing such policies and systems. (See Exhibits 14.15, "Monitoring Employees' Technology Usage," and 14.16, "Allowable Monitoring.")

The Case of Employee E-mail

An employer's need to monitor e-mail must be weighed against an employee's right to privacy and autonomy. The employer is interested in ensuring that the e-mail system is not being used in ways that offend others or harm morale, or for disruptive purposes—a significant concern when two-thirds of employees admit to using e-mail, specifically, for personal reasons having nothing to do with work.[93] Likewise, an employer may choose to review e-mail in connection with a reasonable investigation of possible employee misconduct. Also, companies that maintain sensitive data may be concerned about disclosure of this information by disloyal or careless employees, apparently justifying this type of intrusion.

In a well-publicized case, perhaps because the behavior rose to the highest levels of the organization, the CEO of Boeing resigned amid allegations of unethical conduct. In March 2005, Boeing officials discovered that its CEO, Harry Stonecipher, had transmitted sexually explicit e-mails to another Boeing executive. The case is instructive in that, apparently, Stonecipher and the executive were involved in a consensual relationship and no complaints had been received

Exhibit 14.15 *Monitoring Employees' Technology Usage*

WHY DO FIRMS MONITOR TECHNOLOGY USAGE?

Managing the workplace:

- Ensuring compliance with affirmative action.
- Administering workplace benefits.
- Placing workers in appropriate positions.

Ensuring effective, productive performance:

- Preventing loss of productivity to inappropriate technology use.

Protecting information and guarding against theft.

Protecting investment in equipment and bandwidth.

Protecting against legal liability, including possible

- Perceptions of hostile environments.
- Violations of software licensing laws.
- Violations regarding proprietary information or trade secrets.
- Inappropriate gathering of competitive intelligence.
- Financial fraud.
- Theft.
- Defamation/libel.
- Discrimination.

Maintaining corporate records (including e-mail, voice mail, and so on).

Investigating *some* personal areas. (Consider Infoseek executive Patrick Naughton's pursuit of a tryst with an FBI agent posing as a 13-year-old girl in a chat room.)

ARGUMENTS IN FAVOR OF LIMITS MONITORING

Monitoring may create a suspicious and hostile workplace.

Monitoring constrains effective performance (employees claim that lack of privacy may prevent "flow")

It may be important to conduct *some* personal business at the office, when necessary.

Monitoring causes increased workplace stress and pressure, negatively impacting performance.

Employees claim that monitoring is an inherent invasion of privacy.

Monitoring does not always allow for workers to review and correct misinformation in the data collected.

Monitoring constrains the right to autonomy and freedom of expression.

Monitoring intrudes on one's right to privacy of thought. ("I use a company pen; does that mean the firm has a right to read my letter to my spouse?")

continued

Exhibit 14.15 *continued*

- Consider:
  — Surveys report alarming statistics about the use of the Internet while at work. Among them, up to 40 percent of workplace Internet use is not business-related, 64 percent of workers admit to using the Internet for personal purposes at some point during the workday, and the total amount of time spent on the Web can average more than 18 hours per week.[a]
  — It is estimated that 35 million workers, or approximately 25 percent of U.S. employees, spend an average of 3.5 hours a week on blogs.[b] Men spend a bit more time on nonwork-related Web surfing than women, 2.3 hours per week versus 1.5 hours among women.[c]
  — 13 percent of employees spend over two hours a day surfing nonbusiness sites.[d]
  — 24 percent of employees spend working hours at least one time each week watching or listening to streaming media.[e]
  — 70 percent of all traffic to Internet pornography Web sites is clocked during the traditional working hours of 9:00 a.m. and 5:00 p.m.[f]

[a]Deon Fair et al., "Internet Abuse Continues to Steal Workplace Productivity Despite the Use of Filters," April 27, 2005, http://www.minitrax.com/bw/whitepapers/AIWhitePaper.pdf.

[b]Ezra Palmer, "The Work Force Is Surfing," *I-Media Connection,* October 28, 2005, http://www.imediaconnection.com/content/7068.asp.

[c]Deborah Rothberg, "As Crucial as Coffee: Web Surfing at Work," *e-week,* May 17, 2006, http://www.eweek.com/article2/0,1895,1963997,00.asp. See also Websense, "Web @ Work Survey."

[d]Alan Cohen, "Worker Watchers: Want to Know What Your Employees Are Doing Online? You Can Find Out without Spooking Them," *Fortune/CNET Technology Review,* Summer 2001, pp. 70, 76.

[e]Rothberg, "As Crucial as Coffee."

[f]Staff Monitoring, "Staff Computer and Internet Abuse Statistics," 2007, http://staffmonitoring.com/P32/stats.htm.

Source: Adapted by authors from data from the American Management Association, "2007 Electronic Monitoring & Surveillance Survey," March 13, 2008, www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx

Exhibit 14.16 *Allowable Monitoring*

Telephone calls	Monitoring is permitted in connection with quality control. Notice to the parties to the call is often required by state law, though federal law allows employers to monitor work calls without notice. If the employer realizes that the call is personal, monitoring must cease immediately.
E-mail messages	Under most circumstances, employers may monitor employee e-mails. Even in situations where the employer claims that it will not, its right to monitor has been held to persist. However, where the employee's reasonable expectation of privacy is increased (such as a password-protected account), this may impact the court's decision, though it is not determinative.
Voice mail system messages	Though not yet completely settled, it appears that voice mail system messages are analyzed in the same manner as e-mail messages.
Internet use	Where the employer has provided the equipment and/or the access to the Internet, the employer may track, block, or review Internet use.

from any individuals regarding the relationship. However, Stonecipher was originally hired after Boeing had experienced previous circumstances of alleged wrongdoings and after he, himself, had spearheaded the creation of an ethics policy in response. With notice of the e-mails and the possible later contention that a hostile environment existed for other workers, Boeing executives felt that they had no choice but to ask for his resignation.

While monitoring e-mail transmissions over telephone lines is forbidden by the ECPA, communications within a firm do not generally go over the phone lines and therefore may be legally available to employers. In addition, there are numerous exceptions to the ECPA's prohibitions as discussed earlier in this chapter, including situations where one party to the transmission consents, where the provider of the communication service can monitor communications, or where the monitoring is done in the ordinary course of business. In order to satisfy the ECPA consent exception, however, the employer's interception must not exceed the scope of the employee's consent. Employers must be aware, as well, that an employee's knowledge that the employer is monitoring certain communications is insufficient to be considered implied consent. To avoid liability, employers must specifically inform employees of the extent and circumstances under which e-mail communications will be monitored.

3 Scenario

Despite the failure of legislative attempts to require employers to notify employees that their e-mail is being monitored, such as the proposed Notice of Electronic Monitoring Act, employers should provide such notification, as described below.[94] In addition, some states, including Delaware and Connecticut, have now imposed notice requirements before monitoring.

Developing Computer Use Policies

LO11

An employer can meet its business necessity to monitor e-mail, protect itself from liability, and, at the same time, respect the employees' legitimate expectation of privacy in the workplace in numerous ways. Moreover, research demonstrates that monitoring may be more acceptable to employees when they perceive that monitoring takes place within an environment of procedural fairness and one designed to ensure privacy.[95] Accordingly, employers should develop concise written policies and procedures regarding the use of company computers, specifically e-mail. The Society for Human Resource Management strongly encourages companies both to adopt policies that address employee privacy and to ensure that employees are notified of such policies. Any e-mail policy should be incorporated in the company policies and procedures manuals, employee handbooks, and instruction aids to ensure that the employee receives consistent information regarding the employer's rights to monitor employee e-mail. Additionally, a company could display a notice each time an employee logs on to a company computer indicating the computers are to be used only for business-related communication or explaining that the employee has no reasonable expectation of privacy in the electronic messages. Employers also can periodically send memos reminding employees of the policy. For a sample e-mail, voice mail, and computer systems policy, see Exhibit 14.17, "Sample E-mail, Voice Mail, and Computer Systems Policy."

Exhibit 14.17 *Sample E-mail, Voice Mail, and Computer Systems Policy*

Subject: **E-mail, Voice Mail and Computer Systems Policy**

Purpose: To prevent employees from using the Company computer and voice mail systems for harassing, defamatory, or other inappropriate communications. To preserve the Company's right to monitor and retrieve employee communications. To prohibit excessive personal use of the company's electronic systems.

Related Policies: Other related policies are: Harassment Prevention, Rules of Conduct, Confidentiality of Company Information, Solicitations.

Background: Inappropriate employee use of Company computer, e-mail, and voice mail systems can subject the Company to significant legal exposure. Due to the effervescent nature of computer communications, employees will often say things in e-mail that they would never put in writing. Thus, it is important that all employers have a policy which strongly prohibits the inappropriate use of the Company's electronic systems, and puts employees on notice that the employer reserves the right to monitor such use.

Policy: The Company provides its employees with access to Company computers, network, Internet access, internal and external electronic mail, and voice mail to facilitate the conduct of Company business.

Company Property: All computers and data, information and software created, transmitted, downloaded, or stored on the Company's computer system are the property of Company. All electronic mail messages composed, sent, and received are and remain the property of Company. The voice mail system and all messages left on that system are Company property.

Business Use and Occasional Personal Use: The Company's computers, network, Internet access, electronic mail, and voice mail systems are provided to employees to assist employees in accomplishing their job responsibilities for the Company. Limited occasional personal use of such facilities is acceptable, provided such use is reasonable, appropriate, and complies with this policy. If you have any questions as to whether a particular use of such facilities is permissible, check with your supervisor before engaging in such use. The use of Company's computers, network, Internet access, electronic mail, and voice mail for personal use does not alter the facts that the foregoing remain Company property, and that employees have no reasonable expectation of privacy with respect to such use.

Privacy: Employees shall respect the privacy of others. Except as provided below, messages sent via electronic mail are to be read only by the addressed recipient or with the authorization of the addressed recipient. The data, information and software created, transmitted, downloaded, or stored on the Company's computer system may be accessed by authorized personnel only. Employees should understand that the confidentiality of electronic mail cannot be ensured. Employees must assume that any and all messages may be read by someone other than the intended recipient. Personal passwords are not an assurance of confidentiality. *There is no reasonable expectation of privacy in any e-mail, voice mail, and/or other use of Company computers, network, and systems.*

Prohibited Conduct:

- Employees may not use the Company's computers, network, Internet access, electronic mail, or voice mail to conduct illegal or malicious activities.

continued

- Employees may not transmit or solicit any threatening, defamatory, obscene, harassing, offensive, or unprofessional material. Offensive content would include, but not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of his or her race, religion, color, national origin, ancestry, disability, age, sex, marital status, sexual orientation, or any other class protected by any federal, state, or local law.
- Employees may not create, transmit, or distribute unwanted, mass, excessive or anonymous e-mails, electronic vandalism, junk e-mail, or "spam."
- Employees may not access any Web site that is sexually or racially offensive or discriminatory.
- Employees may not display, download, or distribute any sexually explicit material.
- Employees may not violate the privacy of individuals by any means, such as by reading private e-mails or private communications, accessing private documents, or utilizing the passwords of others, unless officially authorized to do so.
- Employees may not represent themselves as being someone else, or send anonymous communications.
- Employees may not use the e-mail, voice mail, or computer systems to solicit for religious causes, outside business ventures, or personal causes.
- Employees may not transmit any of Company's confidential or proprietary information including (without limitation) customer data, trade secrets, or other material covered by Company's policy re: Confidentiality of Company information.
- Employees may not install, run, or download any software (including entertainment software or games) not authorized by the Company.
- Employees may not disrupt or hinder the use of the Company computers or network, or infiltrate another computer or computing system.
- Employees may not damage software or propagate computer worms or viruses.

Only authorized employees may communicate on the Internet on behalf of the Company.

Monitoring: Company maintains the right to monitor and record employee activity on its computers, network, voice mail and e-mail systems. Company's monitoring includes (without limitation) reading e-mail messages sent to received, files stored or transmitted, and recording Web sites accessed.

Archiving: It is Company's practice to archive (i.e., make backup copies) all electronic documents, files, and e-mail messages incident to the Company's normal back-up procedures. Employees should therefore understand that even when a document, file, or message is deleted, it may still be possible to access that message. Management and law enforcement agencies have the right to access these archives.

Copyright Laws: Any software or other material downloaded into the Company's computers may be used only in ways consistent with the licenses and copyrights of the vendors, authors, and owners of the material. No employee shall make illegal or unauthorized copies of any software or data.

Violations of this Policy: Any violation of this policy may result in disciplinary action up to and including immediate termination. Any employee learning of any violation of this policy should notify his or her [e.g., immediate supervisor] immediately.

continued

Exhibit 14.17 *continued*

Dates: Be sure to date policies when they become effective. Hang on to old policies and be sure to change the date on revised versions.

Source: Lee T. Paterson, ed., *Sample Personnel Policies* (El Segundo, CA: Professionals in Human Resources Association (PIHRA), 2002).

Some experts advocate policies that restrict the use of e-mail to business purposes only and that explain that the employer may access the e-mail both in the ordinary course of business and when business reasons necessitate. If the employer faithfully adheres to this policy 100 percent of the time, this process is certainly defensible. However, such a standard is one that is difficult to honor in every case and the employer may be subject to claims of disparate treatment if applied inconsistently. Therefore, a more realistic approach—and one that is generally accepted in both the courts and common practice—suggests that employees limit their use of technology to reasonable personal access that does not unnecessarily interfere with their professional responsibilities or otherwise unduly impact the workplace financially or otherwise (referring to bandwidth, time spent online, impact on colleagues, and so on).

Kevin Conlon, district counsel for the Communication Workers of America, suggests these additional guidelines that may be considered in formulating an accountable process for employee monitoring:

1. There should be no monitoring in highly private areas such as restrooms.
2. Monitoring should be limited to the workplace.
3. Employees should have full access to any information gathered through monitoring.
4. Continuous monitoring should be banned.
5. All forms of *secret* monitoring should be banned. Advance notice should be given.
6. Only information relevant to the job should be collected.
7. Monitoring should result in the attainment of some business interest.

Philosopher William Parent conceives the right to privacy more appropriately as a right to liberty and therefore seeks to determine the potential affront to liberty from the employer's actions. He suggests the following six questions to determine whether those actions are justifiable or have the potential for an invasion of privacy or liberty:

1. For what purpose is the undocumented personal knowledge sought?
2. Is this purpose a legitimate and important one?
3. Is the knowledge sought through invasion of privacy relevant to its justifying purpose?

4. Is invasion of privacy the only or the least offensive means of obtaining the knowledge?
5. What restrictions or procedural restraints have been placed on the privacy-invading techniques?
6. How will the personal knowledge be protected once it has been acquired?[96]

Both of these sets of guidelines also may respect the personal autonomy of the individual worker by providing for personal space within the working environment, by providing notice of where that "personal" space ends, and by allowing access to the information gathered, all designed toward achievement of a personal and professional development objective.

As is apparent from the above discussion, it is possible to implement a monitoring program that is true to the values of the firm and accountable to those it impacts—the workers. Appropriate attention to the nature and extent of the monitoring, the notice given to those monitored, and the ethical management of the information obtained will ensure a balance of employer and employee interests.

Case 4

In *City of Ontario v. Quon,* included at the end of the chapter, the court examines an employer's decision to monitor employee text message records. As you consider the case, ask yourself whether the employer could have used a less intrusive method for discovering whether the messages were work-related and whether you believe that its stated reason for requesting the records was legitimate.

Blogging and Other Social Media ("Web 2.0")

LO12

social media
User-created content, including text, video, audio, and other multimedia, published in a shared environment, such as a blog, wiki, or other similar site created to enable such sharing

An estimated 200 million blogs were in existence in 2010,[97] a number growing so fast that it was out of date by the time this sentence was written.[98] **Social media** is now the number one activity on the Web (replacing pornography in 2010). But individuals are not the only ones embracing social media; an estimated 80 percent of companies use social media for recruitment, with 95 percent of those using LinkedIn, and more than 700,000 businesses with active pages on Facebook.

The enormous growth in blogging and other social media has created a dilemma for those businesses that have embraced these new technologies. While social media may offer new opportunities to reach a wider customer base in a variety of new ways, it also offers new arenas in which employees can harm the company image, share company information that should not be shared, harass fellow employees, or commit other acts that employers once worried about only with e-mail. A 2007 study by Croner, a British consulting firm, found that an estimated 39 percent of bloggers have made inappropriate comments about their workplace.[99] In a separate survey, 12 percent of U.S. companies reported that they investigated the exposure of confidential or private information posted to a social media site in the previous year.[100]

For better or for worse, social media is here to stay. A 2009 report found a correlation between corporate profitability and engagement in social media, looking at 11 different online social media channels.[101] Generally, those that had a deeper involvement in social media saw revenues grow faster than those that did not.

The challenge for employers now is to find the right balance between embracing social media and discouraging employee misuse. As with e-mail, employers have the right to control what is sent out through the various social media channels it owns. The difficult part is trying to control what employees send out on their own time and through their own social media channels.

In a case included at the end of the chapter and discussed earlier, a San Diego police officer in his free time sold pornographic videos and other paraphernalia, including official police department uniforms, through an adults-only section of eBay. His superiors discovered the activity and ordered him to stop. When he did not, they dismissed him. He sued the department, alleging a violation of his First Amendment right to free speech. Although the appellate court accepted his argument, the U.S. Supreme Court reversed, concluding that the San Diego Police Department had legitimate and substantial interests of its own that were compromised by the employee's speech, especially because the policy officer linked his videos to his work (the videos depicted the police officer in a simulated police uniform).[102] Speech by a public employee that involves "public concern" is entitled to a balancing test, but those that are outside of public concern are subject to tighter restrictions.

The general rule is that bloggers (and other social media users) enjoy First Amendment protections for comments made on blogs and elsewhere; but that protection is not absolute.[103] First, it does not extend to unprotected speech, such as defamation. Second, unless a termination violates an exception, it does not protect employees from the at-will employment doctrine.

The other thing to note is that government employees have even fewer First Amendment rights than private employees. As the Supreme Court said in *Roe*, "a governmental employer may impose certain restraints on the speech of its employees, restraints that would be unconstitutional if applied to the general public."[104]

If employers want to punish employees for statements made in a blog made and posted on their free time, employees have little legal recourse. It has been suggested that they could claim protection under the National Labor Relations Act, if the blogging relates to wages, hours, or working conditions.[105] The fact that NLRA protection is the best that they can hope for illustrates how few protections they have.

Several states have laws that prevent employers from disciplining employees for engaging in lawful conduct away from work, as discussed previously.[106] Those statutes typically refer to "use of a lawful product" and were most often originally designed to prevent employers from punishing employees who smoke or drink *away* from work. Not all the laws are the same; New York, for example, specifically protects off-duty political and recreational activities.

Whether those state laws can be extended to protect blogging activities conducted away from work seems unlikely but remains an open question. Some commentators have suggested that states amend their laws to incorporate protections for off-duty blogging,[107] but none have yet to do so. Until Congress or state legislatures step in, employers will continue to have wide latitude in managing off-duty blogging.

Several cases illustrate the point. Ellen Simonetti was fired in 2004 by Delta Air Lines for an online journal post showing a photograph of her in her Delta uniform. Jessica Cutler was fired in 2004 from her job as a congressional aide after posting blogs detailing her sexual adventures and criticizing her boss. Chez Pazienza was fired in 2008 by CNN for operating a blog without permission. Others have been fired by Starbucks, Microsoft, Wells Fargo, Google, Friendster, the *Washington Post,* and Kmart; and the list goes on. Many of those were fired even though they did not blog in their own name and did not have prior notice that what they were doing would subject them to punishment.

What is an employee to do? The Electronic Frontier Foundation maintains a tutorial on blogging that includes tips on how to avoid getting fired.[108] One key recommendation is to blog anonymously. The Delaware Supreme Court, for example, refused to compel discovery of the identity of an anonymous blogger who published allegedly defamatory comments about a Smyrna, Delaware, city councilman.[109] The ultimate fate of anonymity remains to be seen; but, the court's assertions that "[b]logs and chat rooms . . . are not sources of facts or data upon which a reasonable person would rely," as well as, "readers are unlikely to view messages posted anonymously as assertions of fact," already seem dated.

Until the legal boundaries become clearer, the best possible solution for employers and employees is probably a combination of a clear written policy, some tolerance of criticism, and more effective training. Companies that embrace social media need to find the right balance between encouraging employees to engage in open and honest communications with customers and protecting the company's interests. Therefore, a company social media policy should contain the following:[110]

- **Defined objectives that do not overreach.** A policy can range from restrictive—banning all employee comments on work-related matters, including on their own time—to permissive—allowing contact with customers but warning employees to avoid embarrassing the company.
- **A reminder that company policies apply.** Employers who embrace social media activities should remind employees that company policies continue to apply to off-work social media-related activities, including those involving the sharing of company information, harassment, and discrimination.
- **Personal comment rules.** Employers should establish rules for employees who express opinions through social media; for example, employees who offer personal opinions may be required to identify themselves as employees of the company and provide a disclaimer that they have no authority to speak for the company and that the views are theirs, alone.
- **Disclosure reminders.** If the employer is publicly traded, the policy should include a reminder of the rules imposed by the Securities and Exchange Commission on information disclosures by publicly owned companies.
- **Monitoring reminders.** Employers should remind employees that they retain the right to monitor all social media activities, including the right to view Facebook and Twitter postings made while away from work; they may need to be

reminded that content sent through social media channels is not private and cannot be recalled.

- **Copyright reminders.** Employers may want to include a reminder to respect copyright law; social media users often mistakenly believe that anything they see on the internet is fair game for copying and reusing.

Employers who embrace social media will have to decide how much criticism they are willing to tolerate. Employers that have been willing to tolerate some internal criticisms have sometimes been rewarded for that tolerance with a reputation for open-mindedness and a progressive embrace of social media technologies.

Social media technologies have democratized opinion-giving. Once upon a time, employers could control their message rather effectively by training the few top executives who were authorized to speak for the company. Today, however, any employee with a cell phone or a personal computer can publish her or his opinion any number of ways. Putting such a public microphone in the hands of employees who are untrained in the dangers of misstatements can be disastrous, potentially exposing the company to legal liability and possibly damaging the stock price. The answer is better employee training of the dangers inherent in social media and a clear social media policy that sets forth the employer's expectations of those who intend to use the technologies, including the risks for those who misuse them.

YouTube is another popular social media outlet. Because many cell phones now have not only cameras but also video capabilities, and because many employees carry cell phones, it is a short step between something an employee sees at work and YouTube, or another video-sharing site. Some employers, therefore, have implemented policies banning the use of cameras, cell phones, and any other devices used to take still pictures or video on the theory that employees may not fully appreciate the importance of not sharing the business's inner workings with the rest of the world. Although no cases exist that have challenged such bans, employers are likely within their rights to do so, especially if the ban is tied to a legitimate business reason.

Waivers of Privacy Rights

search
A physical invasion of a person's space, belongings, or body.

waiver
The intentional relinquishment of a known right.

On occasion, an employer may request that an employee waive her or his privacy rights as a condition of employment. This condition could be a **search**. A **waiver** would exempt the employer from liability for claims the employee may have as a result of privacy issues. While a valid waiver must be voluntarily given, requiring a waiver as an employment condition is a questionable approach. Employers maintain a superior bargaining position from which to negotiate such an arrangement, so voluntariness is questionable.

Waivers exist at all stages of employment, from preemployment medical screenings to a waiver of age discrimination claims when being bought out of one's job at an old age. Courts are not consistent in their acceptance of these waivers, but one common link among those that are approved is that there exists

some form of consideration in which the employee receives something in return for giving up rights.

It has thus been held that the waiver at least be accompanied by an offer of employment. No waiver that is given by an applicant prior to a job offer would be considered valid and enforceable. Other requirements articulated by the courts include that the waiver be knowingly and intelligently given and that it be clear and unmistakable, in writing, and voluntary.

Privacy Rights since September 11, 2001

The United States has implemented widespread modifications to its patchwork structure of privacy protections since the terrorist attacks of September 11, 2001. In particular, proposals for the expansion of surveillance and information-gathering authority were submitted and many, to the chagrin of some civil rights attorneys and advocates, were enacted.

The most public and publicized of these modifications was the adoption and implementation of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56. The USA PATRIOT Act expanded states' rights with regard to Internet surveillance technology, including workplace surveillance and amending the Electronic Communications Privacy Act in this regard. The act also grants access to sensitive data with only a court order rather than a judicial warrant, among other changes, and imposes or enhances civil and criminal penalties for knowingly or intentionally aiding terrorists. In addition, the new disclosure regime increased the sharing of personal information between government agencies in order to ensure the greatest level of protection.

Title II of the act provides for the following enhanced surveillance procedures, among others, that have a significant impact on individual privacy and may impact an employer's effort to maintain employee privacy:

- Expanded authority to intercept wire, oral, and electronic communications relating to terrorism and to computer fraud and abuse offenses.
- Provided roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978 (FISA) to track individuals. (FISA investigations are not subject to Fourth Amendment standards but are instead governed by the requirement that the search serve "a significant purpose)."
- Allowed nationwide seizure of voice mail messages pursuant to warrants (i.e., without the previously required wiretap order).
- Broadened the types of records that law enforcement may obtain, pursuant to a subpoena, from electronic communications service providers.
- Permitted emergency disclosure of customer electronic communications by providers to protect life and limb.
- Offered nationwide service of search warrants for electronic evidence.

Management Tips

- Develop and publish policies that reserve your right to monitor, gain access to, or disclose all e-mails in your system. Notify employees of the policy and train all managers (see Exhibit 14.18).
- When developing an e-mail policy, do not overlook instant messaging (IM). Ensure that any policy that applies to e-mails also applies to IMs. IMs can pose a greater security risk than e-mail if the IMs sent to employees are not subject to virus-checking software.
- The same warning applies for the so-called "web 2.0 technologies," such as blogs, social networking, wikis, and similar technologies. Ensure that the privacy policy accounts for these social media technologies and strikes the right balance between appropriate and inappropriate uses.
- The privacy policy should be clear that employees have no expectation of privacy in all employer-provided equipment. Clear policies reduce the likelihood of future disputes.
- As an employer, you may search your employees' property where the employee does not have any expectation of privacy; the difficulty comes in determining where that expectation exists. Therefore, if you believe that searches are necessary, the policy should state clearly where the expectation of privacy ends and under what conditions searches will be permitted.
- Monitoring policies should be clearly stated and should explain that use of technology is subject to review, notwithstanding password protection. They should explain that passwords are provided for the user's protection from external intrusion, as opposed to the creation of an expectation that e-mail is actually private with regard to the employer.
- In designing a monitoring process, avoid content-based and real-time monitoring as both give rise to subjective action rather than standardized procedures and may violate the Federal Wiretap Act.
- Since many privacy protections exist on a state-by-state level, be sure to investigate the specific protections for which you are responsible in the states in which you do business.
- Your privacy policy should be targeted to protect your business interests. Therefore, consider prohibiting the following: (1) the use of cameras, cell phones, or other devices for taking pictures or making recordings on your property, (2) the use of e-mails for distributing illegal or improper content, (3) the use of company trademarks, logos, or other copyrighted material without permission, and (4) the disclosure of company materials to outside entities.
- While it may appear reasonable for you to want to regulate certain off-work activities of your employees, be wary of overrestricting since courts do not look on these regulations positively. Policies regulating off-work activities that have been upheld are generally those that are targeted to protect legitimate business interests, such as the company's reputation.
- On that note, if you do opt to regulate the off-work activities of your employees, you may wish to consider focusing the policy on the possible negative impact of off-duty conduct to the employer's business interests and to the public's perception of the employer, rather than on the specific off-duty conduct, in particular.

- You are less likely to find problems with a waiver of privacy rights where the waiver is accompanied by an offer of employment.
- Ensure that you comply with all privacy rules required by HIPAA, particularly involving the security of employee health records. Train the appropriate employees on those requirements.
- When you do collect personal information about your employees, be sure to regulate access to this information since unwarranted disclosure might constitute an invasion of privacy even where the original collection of information is allowed.
- Technology changes quickly. You should keep abreast of current developments and conduct periodic reviews of the privacy policy to ensure that emerging technologies are covered.
- Ensure that the privacy rules are enforced consistently.

Exhibit 14.18 *Toward Appropriate Information Collection from Employees*

Though it appears that employee privacy might be a moving target, there are steps that employers may take to be respectful of employee information and personal privacy while also maintaining a balanced management of its workplace:

- **First, conduct an information audit** for the purpose of determining those areas of the company's practices and procedures that have the potential for invasion, including what type of information is collected, how that information is maintained, the means by which the information is verified, who has access to the information, and to whom the information is disclosed. The audit should cover all facets of the organization's activities, from recruitment and hiring to termination. In addition, it may be helpful to ascertain what type of information is maintained by different sectors of the organization.
- **Second, in connection with sensitive areas where the company maintains no formal policy, develop a policy** to ensure appropriate treatment of data. It is recommended that a policy and procedure be maintained in connection with the acquisition of information, the maintenance of that information, the appropriate contents of personnel files, the use of the information contained therein, and the conduct of workplace investigations. For instance, in connection with the maintenance of personnel files and the accumulation of personal information about company employees, the employer should request only information justified by the needs of the firm and relevant to employment-related decisions.
- **Third, the information collected should be kept in one of several files maintained on each employee:** (1) a personnel file, which contains the application, paperwork relating to hiring, payroll, and other nonsensitive data; (2) a medical file, which contains physicians' reports and insurance records; (3) evaluation files, which contain any evidence of job performance including, but not limited to, performance appraisals; and (4) a confidential file, which contains data relating to extremely sensitive matters that should not be disclosed except with express and specific authority, such as criminal records or information collected in connection with workplace investigations.
- **Fourth, information should be gathered from reliable sources**, rather than sources of questionable repute such as hearsay and other subjective indicators. Irrelevant or outdated material should periodically be expunged from these records as well.
- **Fifth, publicize privacy policies and procedures, and educate employees** regarding their rights as well as their responsibilities.

Pursuant to these provisions, the government is now allowed to monitor anyone on the Internet simply by contending that the information is "relevant" to an ongoing criminal investigation. In addition, the act provides anti–money-laundering provisions designed to combat money-laundering activity or the funding of terrorist or criminal activity through corporate activity or otherwise. All financial institutions must now report suspicious activities in financial transactions and keep records of foreign national employees, while also complying with anti-discrimination laws discussed throughout this text. It is a challenging balance, claim employers.

The USA PATRIOT Act, set to expire in February 2010, was renewed for one year without including many of the additional privacy measures sought by Democratic lawmakers. One extended provision does allow authorities greater access to certain personal and business records.

The USA PATRIOT Act was not the only legislative response. Both federal and state agencies have passed a number of new pieces of legislation responding to terrorism. Not everyone is comfortable with these protections. Out of concern for the USA PATRIOT Act's permitted investigatory provisions, some librarians now warn computer users in their libraries that their computer use could be monitored by law enforcement agencies (especially since reforms to the act were defeated in 2006 and certain provisions will stay in place for another four years). *The Washington Post* reports that some are even ensuring privacy by destroying records of sites visited, books checked out, and logs of computer use.[111] The American Civil Liberties Union reports that a number of communities have passed Anti–USA PATRIOT Act resolutions.[112]

Employers have three choices in terms of their response to a governmental request for information. They may

1. Voluntarily cooperate with law enforcement by providing, upon request (as part of an ongoing investigation), confidential employee information.
2. Choose not to cooperate and ask instead for permission to seek employee authorization to release the requested information.
3. Request to receive a subpoena, search warrant, or FISA order from the federal agency before disclosing an employee's confidential information.[113]

Chapter Summary

- Privacy is a fundamental right that has been recognized as deserving constitutional protection.
- Public employers are subject to greater scrutiny because their actions are considered to be State actions, thus triggering constitutional protections that generally do not apply to private-sector employers.
- Employee privacy rights in the workplace originate from three sources: the Constitution, various state and federal laws, and the common law; those employees who have employment contracts, either individual or union-negotiated, also have whatever protections are provided in the contracts.
- Common law torts include intrusion into seclusion, public disclosure of private facts, publication in a false light, and defamation.

- Regulation of an employee's off-work activities is a controversial area, with the general rule being that employers have the right to regulate such activity as long as the regulation is connected to a legitimate business interest; some state legislatures have stepped in to limit what employers can regulate.
- Employers generally have the right to monitor employee activity while employees are on employer property; employers are generally are stronger footing if they develop a written policy, they notify employees of the policy, and they enforce the policy consistently.

Chapter-End Questions

1. Can a government employee state a claim for a violation of the constitutional right to privacy when she was required, as a job applicant, to sign an affidavit stating that she had not used tobacco products for one year prior to the application date?
2. A homosexual employee files a claim for invasion of privacy against his employer who shared with co-workers the fact that the employee's male partner was listed on his insurance policy and pension plan as his beneficiary. Does he have a claim?
3. An employee obtains permission to take a leave of absence to attend to a personal matter. A co-worker asks the manager why the employee is on leave. What information may the manager properly share with the co-worker?
4. In March and April 1998, John Doe, an employee of the U.S. Postal Service, missed several weeks of work because of an AIDS-related illness. Doe's supervisor told him that he had to submit an administrative form and a medical certificate explaining why he has sick or he would face disciplinary action for his unexplained absence. He was informed that he may qualify for coverage under FMLA and his supervisor provided him with the appropriate forms to fill out and return. Doe decided to pursue an FMLA request and his physician completed the forms, indicating that Doe had "AIDS related complex" and "chronic HIV infection." Doe submitted the request forms to his employer and, upon his return to work, discovered that his HIV status had become common knowledge among co-workers. Several co-workers made comments to him about his condition and many identified his supervisor as the source of the information. Doe filed a suit against the U.S. Postal Service for violation of the Privacy Act, alleging that Postal Service employees disclosed medical information contained in his FMLA forms. Can Doe prove his case? [*John Doe v. U.S. Postal Service,* No. 01-5395 (DC. Cir. Feb. 7, 2003).]
5. Marriott Resorts had a formal company party for more than 200 employees. At one point during the party, they aired a videotape that compiled employees' and their spouses' comments about a household chore that they hated. However, as a spoof, the video was edited to make it seem as if they were describing what it was like to have sex with their partner. For instance, though the plaintiff's husband (an employee) was actually responding to the question about housework, the plaintiff's husband was quoted on the video as seemingly responding to a provocative question by saying, "the smell. The smell, the smell. And then you go with the goggles. You have to put on the goggles. And then you get the smell through the nose. And as you get into it things start flying all over the place. And the smell. And you get covered in these things." The plaintiff herself was never mentioned by name, nor did she appear on the video. The plaintiff was terribly upset by the video and sued Marriott for intrusion into seclusion and portrayal of facts in a false light. Is Marriott liable? [*Stein v. Marriott Ownership Resorts, Inc.,* 944 P.2d 374 (UT. 1997).][114]

6. An employee submitted an expense report that included costs from a cell phone issued by his company. The company wanted to check the phone to verify information that the employee had provided and, because the employee was in the hospital, they obtained access to his office, as well as a key to his desk drawer, in order to look for the phone. Though they did not find the phone, they did find a pellet gun and ammunition. The employee was fired for violating the employer's weapons ban. Did the supervisors violate the employee's right to privacy? Is the fact that the employee shared the desk with other employees relevant? [*Ratti v. Service Management Systems*, No. 06-6034, DC NJ, 2008.]
7. A company institutes a no-fraternization policy that says that a manager will be fired for dating an hourly employee, regardless of whether the manager is the worker's supervisor. To some, the policy seems overbroad and unnecessary, but is it legal? [*Ellis v. UPS*, 523 F. 3d 823 (7th Cir. 2008).]
8. A trucking company installed in its terminal audio and video devices behind two-way mirrors in both the men's and women's bathrooms. The purpose of the devices was to detect and prevent drug use among the truckers. The devices were discovered when one day the mirror fell off of the wall. Are the tactics used by the trucking company legal because it has a right to restrict drug use? Or is its approach a violation of the truckers' right to privacy? [*Cramer v. Consolidated Freightways Inc.*, 255 F. 3d 683 (9th Cir. 2001).]
9. Two female employees of a 24-hour residential facility for abused and neglected children discovered video recording equipment hidden on a bookshelf in an office that they shared. They were able to lock the door and close the blinds to the office; and one of the women regularly changed clothes there. The California Supreme Court upheld the placement of the hidden video equipment by their employer, even though neither woman was suspected of any wrongdoing. How is that possible? Under what set of facts do you imagine that an employer could permissibly monitor employees who are not suspected of wrongdoing? [*Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272 (2009).]
10. State "sunshine" laws require the release of all documents relating to state business. Are employees' personal e-mails subject to public disclosure? Or do state employees retain privacy in personal e-mails? [*Schill v. Wisconsin Rapids School District*, No. 2008AP967-AC, Wis. Sup. Ct., July 16, 2010.]
11. A management employee had a private office with a locked door. Inside the office was an employer-provided computer, and the employee was told not to use the company computer for personal reasons. He was also warned that his computer use would be monitored. When the company discovered that the employee had child pornography on the computer, it authorized the FBI to go into the office and seize the computer. Given the company's policy, it clearly had the right to monitor the employee's use of the computer. But, what about entering a locked office? Does the employee have an expectation of privacy in the locked office? [*U.S. v. Ziegler*, 474 F. 3d 1184 (9th Cir. 2007).]
12. In June of 1995, a hidden camera and VCR were installed at Salem State College in their off-campus Small Business Development Center. The camera was installed to investigate possible illegal entries into the center after regular business hours. The camera recorded 24 hours a day and was angled to view the entire length of the office, including private areas such as cubicles. During the summer of 1995, Gail Nelson, a secretary at the center, often brought a change of clothes to work and changed in a cubicle, either early in the morning before anyone else was in the office or after work

when the office was empty. These activities were recorded on the hidden camera. When Nelson later learned about the covert surveillance from a co-worker, she filed suit against the college and officials, arguing that they had violated her Fourth Amendment right to privacy. Was this an invasion of privacy? [*Gail Nelson v. Salem State College & others,* SJC-09519 (MA., Dec. 8, 2005–Apr. 13, 2006).] What if the video surveillance had taken place in a back room such as an employee locker area? [*Thompson v. Johnson County Community College,* 930 F. Supp. 501 (D. Kan. 1996), *aff'd,* 108 F.3d 1388 (10th Cir. 1997).]

13. A restaurant employee created a private MySpace page and invited fellow employees to the page for the purpose of sharing work-related frustrations and criticisms of their employer. A manager learned of the page, obtained the password from one of the invited employees, and read the postings. Ultimately, several managers went to the page and read the messages. The employee responsible for the MySpace page was fired. To what extent does an employee have an expectation of privacy in a private MySpace page? Does he have free speech rights to express his opinion to his fellow employees? Did the employer illegally invade his privacy? Is the method the manager used to obtain the password from the employee relevant? In other words, does it make any difference whether he coerced her into giving him the password? [*Pietrylo v. Hillstone Restaurant Group*, 2:06-5754-FSH-PS (D.N.J. 2008).]

End Notes

1. E. J. Bloustein, "Privacy as an Aspect of Human Dignity" in F. D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press 1984), p. 188.
2. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 193 (1890).
3. MacDonald, C., "Why Privacy Matters," *Management Ethics* (Fall/Winter 2010), http://www.ethicscentre.ca/EN/resources/Management_Ethics_FW10_dh.pdf.
4. See, for example, Avner Levin, "Dignity in the Workplace: An Enquiry into the Conceptual Foundation of Workplace Privacy Protection Worldwide," *ALSB Journal of Employment and Labor Law* 11, no. 1, p. 63 (Winter 2009).
5. an-Noor 24, pp. 27–28 (Yusufali); al-Hujraat 49, pp. 11–12 (Yusufali).
6. Vol. 1, Book 10, no. 509 (Sahih Bukhari); Book 31, no. 4003 (Sunan Abu Dawud).
7. R. L. Wakefield, "Computer Monitoring and Surveillance: Balancing Privacy with Security," *CPA Journal* 74, no. 7 (2004), pp. 52–55.
8. Delia Fahmy, "More U.S. Employers Testing Workers for Drug Use," *International Herald Tribune,* May 10, 2007, http://www.iht.com/articles/2007/05/10/business/drugtests.php (last visited August 5, 2007).
9. Deloitte & Touche, Poneman Institute, LLC, "Enterprise @ Risk: 2007 Privacy & Data Protection Survey," December 12, 2007, http://www.deloitte.com/dtt/article/0%2C1002%2Ccid%25253D182733%2C00.html.
10. 381 U.S. 479 (2965).
11. Steve Ulfelder, "CPOs on the Rise?" *Computerworld,* March 15, 2004, http://www.computerworld.com/securitytopics/security/story/0.10801.91166.00.html, quoting Alan F. Westin, president of the nonprofit Privacy & American Business organization.

12. See, for example, *Smyth v. Pillsbury*, 914 F.Supp. 97 (E.D. Penn. 1996). The standard was first enunciated in by the U.S. Supreme Court in *Katz v. U.S.*, 389 U.S. 347 (1967), a Fourth Amendment search and seizure case involving a public telephone booth.
13. *Ulrich v. K-Mart*, 858 F.Supp. 1087 (D. Kan. 1994).
14. 795 F.2d 1136, 1141 (3d Cir. 1986).
15. 489 U.S. 602, 109 S. Ct. 1402 (1989), *aff'd,* 934 F.2d 1096 (9th Cir. 1991).
16. *U.S. v. Slanina,* 283 F.3d 670 (5th Cir. 2002); *Leventhal v. Knapek,* 266 F.3d 64 (2d Cir. 2001).
17. 474 F.3d 1184 (9th Cir. 2007), http://bulk.resource.org/courts.gov/c/F3/474/474.F3d.1184.05-30177.html.
18. As an interesting side note, though U.S. law considers child pornography illegal, most states have no legal obligation to report it. Only Arkansas, Missouri, Oklahoma, South Carolina, and South Dakota have laws that require workers in the information technology arena to report child pornography when it is found on workers' computers. Tam Harbert, "Dark Secrets and Ugly Truths: When Ethics and IT Collide," *Computerworld,* September 12, 2007.
19. *Ziegler,* 474 F.3d at 1199.
20. 18 U.S.C. §§ 2510–2521.
21. *Annual Report on Wiretapping in the U.S.*, Administrative Office of the United States Courts, p. 6, April 2010; www.scribd.com/doc/30800548/Annual-Report-on-Wiretapping-in-the-U-S.
22. *Fraser v. National Mutual Insurance,* 352 F.3d 107 (3d Cir. 2003). See also *United States v. Steiger,* 318 F.3d 1039 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868 (9th Cir. 2002); and *Steve Jackson Games, Inc. v. U.S. Secret Serv.,* 36 F.3d 457 (5th Cir. 1994).
23. Montana is the one exception. Employees can be fired only for good cause under the Wrongful Discharge from Employment Act, Mont. Code Ann. §39-2-901, et seq. (2008).
24. 50 S.E. 68 (Ga. 1905).
25. *Lake v. Wal-Mart Stores, Inc.,* 582 N.W.2d 231 (Minn. 1998).
26. 526 F. Supp. 523 (D.D.C. 1981).
27. 66 Md. App. 133, 502 A.2d 1101, cert. denied, 306 Md. 289, 508 A.2d 488, cert. denied, 479 U.S. 984 (1986).
28. 561 F. Supp. 872 (S.D. Ga. 1983).
29. Certain states, however, provide no statutory protection, including Alabama, Connecticut, Mississippi, Nebraska, New Jersey, New York, Vermont, and Washington.
30. As of publication, these included Arizona, Connecticut, the District of Columbia, Illinois, Indiana, Kentucky, Louisiana, Maine, Mississippi, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Virginia, West Virginia, and Wyoming. See also John Pearce and Dennis Kuhn, "The Legal Limits of Employees' Off-Duty Privacy Rights," *Organizational Dynamics* 32, no. 4 (2003), pp. 372–83 and Ariana R. Levinson, "Industrial Justice: Privacy Protection for the Employed," *Cornell Journal of Law and Public Policy*, Vol. 18, p. 609 (2009).
31. R. Parekh, "States Hit Public Employees with Smoking Surcharge," *Business Insurance,* May 23, 2005.

32. M. McDonough, "Whirlpool Plant Suspends 39 Employees Caught Smoking," *ABA Journal,* April 23, 2008, http://www.abajournal.com/news/whirlpool_plant_suspends_39_employees_caught_smoking/; J. Wojcik, "Smoke Gets in Your Lies," *Workforce Week,* April 22, 2008, http://www.workforce.com/section/00/article/25/49/15.html.
33. D. Costello, "Workers Are Told to Shape up or Pay up," *Los Angeles Times,* July 29, 2007, http://www.latimes.com/news/nationworld/nation/la-fi-obese29jul29,1,7252935.story?coll=la-headlines-nation&ctrack=3&cset=true.
34. SHRM Research, "2006 Workplace Romance Poll Finding."
35. Ibid.
36. 237 F.3d 166 (2d Cir. 2001).
37. C. Boyd, "The Debate over the Prohibition of Romance in the Workplace," *Journal of Business Ethics,* v. 97 (2010), p. 325.
38. J. T. A. Gabel, and N. R. Mansfield, "The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace," *American Business Law Journal* 40 (2003), pp. 301–51.
39. Mike Brunker, "Cyberporn Nurse: I Feel Like Larry Flynt," MSNBC, July 16, 1999.
40. CCH Human Resources Workforce Online, *Do Workplace Smoking Laws Regulate Your Business?*http.//www.workforceonline.com/section/03/0005085.htm.
41. Electronic Privacy Information Center, "Workplace Privacy" (2010), http://epic.org/privacy/workplace/ (accessed November 27, 2010).
42. American Management Association, "Electronic Monitoring and Surveillance 2007 Survey."
43. Philip Gordon, and Katherine C. Franklin, "Blogging and the Workplace," *Law.com,* August 8, 2006.
44. Proofpoint, Inc., "Outbound Email and Data Loss Prevention in Today's Enterprise," 2008; survey conducted by Forrester Consulting.
45. *The Urban Dictionary,*http://www.urbandictionary.com/define.php?term=dooced.
46. Graeme Smith, "Is Big McBrother Invading Workplace Privacy?" *The Globe and Mail,* January 13, 2004, p. A8.
47. Philip Gordon, "It's 11 a.m. Do You Know Where Your Employees Are? Effective Use of Location-Based Technologies in the Workplace," 2005, http://library.findlaw.com/2005/Mar/10/163970.html.
48. See, for example, William A. Herbert and Amelia K. Tuminaro, "The Impact of Emerging Technologies in the Workplace: Who's Watching the Man (Who's Watching Me)?," 25:355 *Hofstra Labor & Employment Law Journal* (2009).
49. Wis. Stat. Ann. §146.25.
50. Herbert and Tuminaro, supra, at p. 386.
51. According to "Telework Trendlines 2009," a survey by WorldatWork in conjunction with The Dieringer Research Group Inc.
52. Ashley Benigno, "Total Surveillance Is Threatening Your Health," *Asian Labour Update* (Hong Kong: Asia Monitor Resource Center, http://www.amrc.org.hk/Arch/3405.htm, last visited February 5, 2002).
53. Richard Rosenberg, "The Technological Assault on Ethics in the Modern Workplace," in *The Ethics of Human Resources and Industrial Relations,* ed. John W. Budd and James G. Scoville (Champaign, IL: Labor and Employment Relations Assn., 2005).

54. U. Klotz, "The Challenges of the New Economy," October 1999, cited in *World Employment Report 2001: Life at Work in the Information Economy,* p. 145 (Geneva: International Labour Office, 2001).
55. Tam Harbert, "Dark Secrets and Ugly Truths: When Ethics and IT Collide," *Computerworld,* September 12, 2007.
56. Colin Bennett, "Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web," *Ethics and Information Technology* 3 (2001), pp. 197–210.
57. Ethisphere, "Mesa Airlines CFO Scrambled to Erase Porn," September 27, 2007, http://ethisphereblog.com/mesa-airlines-cfo-scrambled-to-erase-porn-not-valuable-evidence/#more-1273 (last visited September 28, 2007).
58. Dana Hawkins, "Lawsuits Spur Rise in Employee Monitoring," *U.S. News & World Report,* August 13, 2001.
59. Ibid.
60. Andrew Schulman, "One-Third of U.S. Online Workforce under Internet/Email Surveillance," *Workforce Surveillance Project* (Privacy Foundation), July 9, 2001, http://www.privacyfoundation.org/workplace/business/biz_show.asp?id=70&ac.
61. Jeffrey Benner, "Privacy at Work? Be Serious," *Wired Magazine,* March 2001, http://www.wired.com/news/business/0,1367,42029,00.html (accessed February 26, 2002).
62. Pew Internet and American Life Project, *How Americans Use Instant Messaging,* September 1, 2004, p. 2, http://www.pewinternet.org.
63. http://www.omnitracs.com.
64. http://www.spyzone.com.
65. American Management Association, "Electronic Monitoring and Surveillance 2007 Survey."
66. American Civil Liberties Union, "Privacy in America: Electronic Monitoring," December 31, 1997, http://www.aclu.org/privacy/workplace/15104res19971231.html (last visited July 26, 2007).
67. American Management Association and the ePolicy Institute, "2005 Electronic Monitoring & Surveillance Survey."
68. *Scott v. Beth Israel Medical Center, Inc.,* 847 N.Y.S.2d 436 (2007); but see, contra, *Curto v. Medical World Communications, Inc.,* 2006 WL 1318387 (E.D.N.Y. 2006).
69. R. Hollinger and L. Langton, "2005 National Retail Security Survey," 2005, http://www.crim.ufl.edu/research/srp/finalreport_2005.pdf.
70. Hayes International, 18th Annual Retail Theft Survey, http://www.hayesinternational.com/ts_emply_thft.html (last visited July 25, 2007).
71. Karen Robinson-Jacobs, "Retailers Taking Aim at Employee Pilferage," *Los Angeles Times,* February 16, 2002, p. C1.
72. *Shoars v. Epson America, Inc.,* No. SCW 112749 (Cal. Super. Ct., L.A. Cty., 1990), *appeal denied,* 994 Cal. LEXIS 3670 (Cal. 1994); James McNair, "When You Use E-mail at Work, Your Boss May Be Looking In," *Telecom Digest,*http://icg.stwing.upenn.edu/cis500/reading.062.htm, reprinted from the *Miami Herald,* February 9, 1994.
73. Winn Schwartau, "Who Controls Network Usage Anyway?" *Network World,* May 22, 1995, p. 71.
74 Bureau of National Affairs, "Northern Telecom Settles with CWA on Monitoring," *Individual Employment Rights,* March 10, 1992, p. 1.

75. 59 Cal. Rptr. 2d 834 (Cal. Ct. App. 1996).
76. See Ted Clark, "Legal Corner: Monitoring Employee Activities: Privacy Tensions in the Public Workplace," *NPLERA Newsletter,* June 1999, http://www.seyfarth.com/practice/labor/articles/II_1393.html.
77. Lisa Reed and Barry Freidman, "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use," *Employee Responsibilities and Rights Journal* 19, no. 2 (June 2007), pp. 75–83.
78. 2004 U.S. Dist. LEXIS 18863 (D. Or. 2004).
79. 18 U.S.C. §§ 2510–2520.
80. See, for example, Galit Kierkut and Suzanne M. Cerra, "Monitoring Electronic Communications and Social Media Usage in the Workplace: What are the Limits?" *New Jersey Labor and Employment Law Quarterly* 32, no.2 (2010).
81. 201 N.J. 300 March 30, 2010).
82. 2008 WL 3128429 (D.N.J. July 25, 2008).
83. See Frederic Lardinois, "Want to Work for the City of Bozeman, MT? Hand Over Your Social Network Logins and Passwords," ReadWriteWeb, June 18, 2009, www.readwriteweb.com/archives/want_to_work_for_the_city_of_bozeman_mt_hand_over_passwords_login_info.php.
84. *EEOC v. Simply Storage Management,* case no. 2010 U.S. Dist., LEXIS 527661, 1:09-cv-1223-WTL-DML (SD. IN., 5/11/2010), http://www.scribd.com/doc/31921843/EEOC-v-Simply-Storage-Mgmt-LLC.
85. 382 N.J. Super. 122, 887 A. 2d 1156 (App. Div. 2005).
86. Alan Cohen, "Worker Watchers: Want to Know What Your Employees Are Doing Online? You Can Find Out without Spooking Them," *Fortune/CNET Technology Review,* Summer 2001, p. 70.
87. Ibid.
88. Proofpoint, Inc., "Outbound Email and Data Loss Prevention in Today's Enterprise," 2008; survey conducted by Forrester Consulting.
89. *Harley v. McCoach,* 928 F. Supp. 533 (E.D. Pa. 1996), cited in "Cyberliability: An Enterprise White Paper," Elron Software, http://www.internetmanager.com.
90. 217 F.R.D. 309, 312 (S.D.N.Y. 2003); see also "Jury Awards $29.2 Million in Damages to Discharged Equities Saleswoman," *Daily Labor Report* (BNA), April 13, 2005, p. 449.
91. Cohen, "Worker Watchers," p. 76.
92. Dan Charles, "High-Tech Equipment in the Workplace," *All Things Considered,* National Public Radio, April 1, 1996.
93. Websense, "Web @ Work Survey," 2006, http://www.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/?Release=0605161213.
94. Christopher A. Weals, "Workplace Privacy," *Legal Times,* March 6, 2002.
95. Reed and Freidman, "Workplace Privacy," pp. 75–83.
96. Miriam Schulman, "Little Brother Is Watching You," *Issues in Ethics* 9, no. 2 (Spring 1998).
97. See samswebguide.com/2010/07/13/60-amazing-blogging-social-media-statistics-facts-revealed.
98. Real Time Statistics project, http://www.worldometers.info/ (2010).
99. See Bloggers @ Work, www.justia.com/employment/docs/boggers-at-work.html.

100. Proofpoint, Inc., "Outbound Email and Data Loss Prevention in Today's Enterprise," 2008; survey conducted by Forrester Consulting.
101. The Altimeter Group, www.altimeter.com/2009/07/engagementdb.html. The 11 channels were: blogs, branded social networks, content distribution to other sites, discussion forums, external social network presences (Facebook, MySpace), Flickr/Photobucket, innovation hubs, wikis, ratings and reviews, Twitter, and YouYube.
102. *City of San Diego v. Roe,* 543 U.S. 77 (2004).
103. See, for example, Tracie Watson and Elisabeth Piro, "Bloggers Beware: A Cautionary Tale of Blogging and the Doctrine of At-Will Employment," 24:333 *Hofstra Labor & Employment Law Journal,* p. 358, Aug. 30, 2007.
104. *City of San Diego,* supra.
105. See Christine E. Howard, "Invasion of Privacy Liability in the Electronic Workplace: A Lawyer's Perspective," 25:511 *Hofstra Labor & Employment Law Journal,* p. 517, Feb. 4, 2009.
106. See, for example, New York Consolidated Law §7-201-d (2009); Minn. Stat. §181.938 (2009); Mont. Code Ann. §39-2-313 (2009); Nev. Rev. Stat. §613.333 (2009); N.C. Gen. Stat. §95-28.2 (2009); Tenn. Code Ann. §50-1-304(e) (2009).
107. See, for example, Arianna R. Levinson, "Industrial Justice: Privacy Protection for the Employed," *Cornell Journal of Law and Public Policy,* Vol. 18, p. 609 (2009).
108. www.eff.org/wp/blog-safely.
109. *Doe v. Cahill,* 884 A.2d 451 (Del. 2005).
110. Adapted from Robert Barnes and Darya V. Pollak, "Employees Online: Protecting Company Interests in a Web 2.0 World," Bloomberg Finance L.P. (Nov. 10, 2008).
111. Rene Sanchez, "Librarians Make Some Noise over Patriot Act," *The Washington Post,* April 10, 2003, p. A20.
112. http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11256&c=206.
113. Vance Knapp, "The Impact of the Patriot Act on Employers," 2003, http://www.rothgerber.com/newslettersarticles/le0024.asp.
114. http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=ut&vol=appopin&invol=stien.

Cases

O'Connor v. Ortega *480 U.S. 709 (1987)*

The respondent, Dr. Ortega, was a physician and psychiatrist and an employee of a state hospital who had primary responsibility for training physicians in the psychiatric residency program. Hospital officials became concerned about possible improprieties in his management of the program. In particular, the officials thought that Dr. Ortega may have misled the hospital into believing that the computer had been donated when, in fact, the computer had been financed by the possibly coerced contributions of residents. Hospital officials were also concerned about charges that Dr. Ortega had sexually harassed two female hospital employees, and that he had taken inappropriate disciplinary action against a resident.

While he was on administrative leave pending investigation of the charges, hospital officials, allegedly in order to inventory and secure state property, searched Dr. Ortega's office and took personal items from his desk and file cabinets that later were used in administrative proceedings resulting in his discharge. The employee filed an action against the hospital officials, alleging that the search of his office violated the Fourth Amendment. The trial court found that the search was proper in order to secure state property. The court of appeals held that the employee had a *reasonable expectation of privacy* in his office, and thus the search violated the Fourth Amendment. The Supreme Court explains that a search must be reasonable both from its inception as well as in its scope, and remands the case to the district court for review of the reasonableness of both of those questions.

O'Connor, J.

***

Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. The workplace includes those areas and items that are related to work and are generally within the employer's control. At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board.

Not everything that passes through the confines of the business address can be considered part of the workplace context, however. . . . The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address.

***

Given the societal expectations of privacy in one's place of work, we reject the contention made by the Solicitor General and petitioners that public employees can never have a reasonable expectation of privacy in their place of work. Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the workplace, however, may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation. The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others—such as fellow employees, supervisors, consensual visitors, and the general public—may have frequent access to an individual's office. . . .

The undisputed evidence discloses that Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos.

The files on physicians in residency training were kept outside Dr. Ortega's office. Indeed, the only items found by the investigators were apparently personal items because, with the exception of the items seized for use in the administrative hearings, all the papers and effects found in the office were simply placed in boxes and made available to Dr. Ortega. Finally, we note that there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or file cabinets, although the absence of such a policy does not create an expectation of privacy where it would not otherwise exist.

On the basis of this undisputed evidence, we accept the conclusion of the Court of Appeals that Dr. Ortega had a reasonable expectation of privacy at least in his desk and file cabinets.

Having determined that Dr. Ortega had a reasonable expectation of privacy in his office, . . . we must determine the appropriate standard of reasonableness applicable to the search. A determination of the standard of reasonableness applicable to a particular class of searches requires "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.

***

The governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace. Government agencies provide myriad services to the public, and the work of these agencies would suffer if employers were required to have probable cause before they entered an employee's desk for the purpose of finding a file or piece of office correspondence. Indeed, it is difficult to give the concept of probable cause, rooted as it is in the criminal investigatory context, much meaning when the purpose of a search is to retrieve a file for work-related reasons. Similarly, the concept of probable cause has little meaning for a routine inventory conducted by public employers for the purpose of securing state property. To ensure the efficient and proper operation of the agency, therefore, public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons.

We come to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct. Even when employers conduct an investigation, they have an interest substantially different from "the normal need for law enforcement." Public employers have an interest in ensuring that their agencies operate in an effective and efficient manner, and the work of these agencies inevitably suffers from the inefficiency, incompetence, mismanagement, or other work-related misfeasance of its employees. Indeed, in many cases, public employees are entrusted with tremendous responsibility, and the consequences of their misconduct or incompetence to both the agency and the public interest can be severe. . . . Public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner. In our view, therefore, a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers. The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest. Additionally, while law enforcement officials are expected to "schoo[l] themselves in the niceties of probable cause," no such expectation is generally applicable to public employers, at least when the search is not used to gather evidence of a criminal offense. It is simply unrealistic to expect supervisors in most government agencies to learn the subtleties of the probable cause standard. . . .

Balanced against the substantial government interests in the efficient and proper operation of the workplace are the privacy interests of government employees in their place of work which, while not insubstantial, are far less than those found at home or in some other contexts. . . . The employer intrusions at issue here "involve a relatively limited invasion" of employee privacy. Government offices are provided to employees for the sole purpose of facilitating the work of an agency. The employee may avoid exposing personal belongings at work by simply leaving them at home.

. . . We hold . . . that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable:

> Determining the reasonableness of any search involves a twofold inquiry: first, one must consider "whether the … action was justified at its inception,"

> second, one must determine whether the search as actually conducted "was reasonably related in scope to the circumstances which justified the interference in the first place."

Ordinarily, a search of an employee's office by a supervisor will be "justified at its inception" when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file. Because petitioners had an "individualized suspicion" of misconduct by Dr. Ortega, we need not decide whether individualized suspicion is an essential element of the standard of reasonableness that we adopt today. The search will be permissible in its scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."

***

On remand, therefore, the District Court must determine the justification for the search and seizure, and evaluate the reasonableness of both the inception of the search and its scope.

Accordingly, the judgment of the Court of Appeals is REVERSED and the case is REMANDED to that court for further proceedings consistent with this opinion.

Case Questions

1. Do you think the standard of the search articulated in this opinion is the correct standard for determining whether a search violates the Fourth Amendment? Think of arguments for both perspectives—the employer and employee.
2. How can an employer protect itself from a claim of an unreasonable search conducted in the workplace? Note the court stated that a policy regarding this issue was not a determinative factor in determining the constitutionality of the search.
3. What could you do as an employee to protect yourself from a company search?

Yoder v. Ingersoll-Rand Company a.k.a. ARO

31 F. Supp. 2d 565 (W.D. Ohio 1997)

Lavern Yoder sued his employer, Ingersoll-Rand Company, to recover for damages he alleged were caused as a result of the employer's failure to keep his medical records confidential. Yoder was employed as a tow motor driver. After he learned that he was HIV-positive, Yoder made every effort to keep his HIV-positive status confidential from his employer because he was concerned that he might suffer adverse employment consequences if his employer or co-workers learned of his condition. A year and a half later, his doctor recommended that he take a medical leave of absence because of stress-induced asthma. An employment disability form was sent by mistake through the employer's mail system, through inner office mail, and then finally to Yoder's home, where it was read by his mother. She learned from the Physician's Statement that he had AIDS. She had known her son was HIV-positive but did not know he had AIDS. Yoder brought a complaint against the firm for permitting the unauthorized disclosure of his medical condition. Count four alleged state common-law claim for invasion of privacy. Both sides moved for summary judgment.

Katz, J.

***

E. Invasion of Privacy

Yoder alleges an invasion of privacy under the theory, public disclosure of private facts about the plaintiff with which the public has no legitimate concern, which is also known as the "publicity" tort. In order successfully to make out a claim under the "publicity" prong, Plaintiff must show five elements:

(1) there must be publicity, i.e., the disclosure must be of a public nature, not private;

(2) the facts disclosed must be those concerning the private life of an individual, not his public life;

(3) the matter publicized must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities;
(4) the publication must have been made intentionally, not negligently; and
(5) the matter publicized must not be a legitimate concern to the public.

Plaintiff can show neither the first nor the fourth element of this test. As to the first element, Plaintiff can prevail only if he shows that the matter has been communicated to "the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." It is not enough to show merely that the matter was communicated by the defendant to a third person. The record evidence indicates that Plaintiff's HIV/AIDS status was actually communicated to only one unauthorized person. Even if the Court accepts Plaintiff's argument that mail clerk Kornrumpf and supervisor Chroninger should be treated as having received the information because they had the opportunity to read Plaintiff's medical report, the information was communicated to three people at most. Three people do not constitute "the public at large." Plaintiff cannot meet the publicity prong of the test.

As to the fourth element, Plaintiff cannot show that Defendant, or its authorized agents, made the disclosure intentionally, even as to Plaintiff's mother. It is undisputed that nothing on the outside of the envelope received in the ARO mail room indicated that it contained a confidential medical record. Kornrumpf's testimony that she did not read the form beyond Plaintiff's name, and did not know that it was a confidential medical record, is undisputed. Chroninger's testimony that he did not read the form, and did not know that it was a confidential medical record, is undisputed. It is a logical impossibility for a party intentionally to disclose information that it does not know it has. Furthermore, the disclosure would not have occurred without Plaintiff's mother's intervening act of opening and reading the medical records without authorization from Defendant. Plaintiff cannot meet the intent prong of the test. Defendant's motion for summary judgment on Count IV is granted.

***

Plaintiff's motion for summary judgment is DENIED. Defendant's motion for summary judgment is GRANTED.

Case Questions

1. Do you think Yoder should have prevailed on his state law claim of invasion of privacy? Why or why not?
2. Do you think this case would have been decided differently if the mail clerk and Yoder's supervisor did read the doctor's statements?
3. How many people would have to read a sensitive document such as this to meet the public disclosure requirement for an individual to prevail on his or her claim?

City of San Diego v. Roe, *543 U.S. 77 (2004)*

The City of San Diego terminated a police officer for selling homemade, sexually explicit videotapes and related activities. Using an adults-only section of eBay, the officer sold not only videotapes of himself in a police uniform but also official San Diego Police Department uniforms and other police equipment. The officer sued the city, alleging a violation of his First Amendment right to free speech. The trial court found for the city on the ground that the speech was not entitled to protection because it was not of "public concern." The Ninth Circuit, however, reversed the trial court, finding that his conduct fell within the protected category of citizen commentary on matters of public concern because it took place off-duty, it was away from the employer's premises, and it did not involve a workplace grievance. The U.S. Supreme Court reversed.

Per Curiam

***

A government employee does not relinquish all First Amendment rights otherwise enjoyed by citizens just by reason of his or her employment. On the other hand, a governmental employer may impose certain restraints on the speech of its employees, restraints that would be unconstitutional if applied to the general public. The

Court has recognized the right of employees to speak on matters of public concern, typically matters concerning government policies that are of interest to the public at large, a subject on which public employees are uniquely qualified to comment. Outside of this category, the Court has held that when government employees speak or write on their own time on topics unrelated to their employment, the speech can have First Amendment protection, absent some governmental justification "far stronger than mere speculation" in regulating it. *United States v. Treasury Employees* (NTEU). We have little difficulty in concluding that the City was not barred from terminating Roe under either line of cases.

In concluding that Roe's activities qualified as a matter of public concern, the Court of Appeals relied heavily on the Court's decision in NTEU. In NTEU it was established that the speech was unrelated to the employment and had no effect on the mission and purpose of the employer. The question was whether the Federal Government could impose certain monetary limitations on outside earnings from speaking or writing on a class of federal employees. The Court held that, within the particular classification of employment, the Government had shown no justification for the outside salary limitations. The First Amendment right of the employees sufficed to invalidate the restrictions on the outside earnings for such activities. The Court noted that throughout history public employees who undertook to write or to speak in their spare time had made substantial contributions to literature and art, and observed that none of the speech at issue "even arguably [had] any adverse impact" on the employer.

The Court of Appeals' reliance on NTEU was seriously misplaced. Although Roe's activities took place outside the workplace and purported to be about subjects not related to his employment, the SDPD demonstrated legitimate and substantial interests of its own that were compromised by his speech. Far from confining his activities to speech unrelated to his employment, Roe took deliberate steps to link his videos and other wares to his police work, all in a way injurious to his employer. The use of the uniform, the law enforcement reference in the Web site, the listing of the speaker as "in the field of law enforcement," and the debased parody of an officer performing indecent acts while in the course of official duties brought the mission of the employer and the professionalism of its officers into serious disrepute.

The Court of Appeals noted the City conceded Roe's activities were "unrelated" to his employment. In the context of the pleadings and arguments, the proper interpretation of the City's statement is simply to underscore the obvious proposition that Roe's speech was not a comment on the workings or functioning of the SDPD. It is quite a different question whether the speech was detrimental to the SDPD. On that score the City's consistent position has been that the speech is contrary to its regulations and harmful to the proper functioning of the police force. The present case falls outside the protection afforded in NTEU. The authorities that instead control, and which are considered below, are this Court's decisions in *Pickering, Connick,* and the decisions which follow them.

To reconcile the employee's right to engage in speech and the government employer's right to protect its own legitimate interests in performing its mission, the Pickering Court adopted a balancing test. It requires a court evaluating restraints on a public employee's speech to balance "the interests of the [employee], as a citizen, in commenting upon matters of public concern and the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees."

Underlying the decision in *Pickering* is the recognition that public employees are often the members of the community who are likely to have informed opinions as to the operations of their public employers, operations which are of substantial concern to the public. Were they not able to speak on these matters, the community would be deprived of informed opinions on important public issues. The interest at stake is as much the public's interest in receiving informed opinion as it is the employee's own right to disseminate it.

Pickering did not hold that any and all statements by a public employee are entitled to balancing. To require *Pickering* balancing in every case where speech by a public employee is at issue, no matter the content of the speech, could compromise the proper functioning of government offices. This concern prompted the Court in *Connick* to explain a threshold inquiry (implicit in Pickering itself) that in order to merit Pickering balancing, a public employee's speech must touch on a matter of "public concern."

In *Connick,* an assistant district attorney, unhappy with her supervisor's decision to transfer her to another division, circulated an intraoffice questionnaire. The document solicited her co-workers' views on, inter alia, office transfer

policy, office morale, the need for grievance committees, the level of confidence in supervisors, and whether employees felt pressured to work in political campaigns.

Finding that—with the exception of the final question—the questionnaire touched not on matters of public concern but on internal workplace grievances, the Court held no Pickering balancing was required. To conclude otherwise would ignore the "common-sense realization that government offices could not function if every employment decision became a constitutional matter." *Connick* held that a public employee's speech is entitled to Pickering balancing only when the employee speaks "as a citizen upon matters of public concern" rather than "as an employee upon matters only of personal interest."

Although the boundaries of the public concern test are not well-defined, Connick provides some guidance. It directs courts to examine the "content, form, and context of a given statement, as revealed by the whole record" in assessing whether an employee's speech addresses a matter of public concern. In addition, it notes that the standard for determining whether expression is of public concern is the same standard used to determine whether a common-law action for invasion of privacy is present. That standard is established by our decisions in *Cox Broadcasting Corp. v. Cohn,* and *Time, Inc. v. Hill*. These cases make clear that public concern is something that is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public at the time of publication. The Court has also recognized that certain private remarks, such as negative comments about the President of the United States, touch on matters of public concern and should thus be subject to Pickering balancing.

Applying these principles to the instant case, there is no difficulty in concluding that Roe's expression does not qualify as a matter of public concern under any view of the public concern test. He fails the threshold test and Pickering balancing does not come into play.

Connick is controlling precedent, but to show why this is not a close case it is instructive to note that even under the view expressed by the dissent in *Connick* from four Members of the Court, the speech here would not come within the definition of a matter of public concern. The dissent in *Connick* would have held that the entirety of the questionnaire circulated by the employee "discussed subjects that could reasonably be expected to be of interest to persons seeking to develop informed opinions about the manner in which . . . an elected official charged with managing a vital governmental agency, discharges his responsibilities." No similar purpose could be attributed to the employee's speech in the present case. Roe's activities did nothing to inform the public about any aspect of the SDPD's functioning or operation. Nor were Roe's activities anything like the private remarks at issue in *Rankin,* where one co-worker commented to another co-worker on an item of political news. Roe's expression was widely broadcast, linked to his official status as a police officer, and designed to exploit his employer's image.

The speech in question was detrimental to the mission and functions of the employer. There is no basis for finding that it was of concern to the community as the Court's cases have understood that term in the context of restrictions by governmental entities on the speech of their employees.

Case Questions

1. In your opinion, does the Ninth Circuit's conclusion that Roe's activities were protected by the First Amendment have merit?
2. Where do you think the line would have drawn on Roe's free speech rights by the Supreme Court had he not tied his activities to the police department? What if Roe did not wear a police uniform but still sold police-related paraphernalia? What if he wore a police uniform but did not sell police-related paraphernalia?
3. Is the "public concern" requirement from the *Pickering* case a fair balancing of the rights involved? How might it be improved?

City of Ontario v. Quon, *130 S. Ct. 2619 (2010)*

The City of Ontario, California, acquired pagers that could send and receive text messages. The pagers were issued to Quon and other police officers, who were told that the city-provided service plan provided a monthly limit on the number of characters sent and received each month. Overages had to be paid by the employees. When the employees exceeded their monthly limits for several months, the police chief sought to determine if the overages being paid by the police officers were for city-related business or personal messages. Based on transcripts sent by the service provider, the police chief discovered that Quon had been sending sexually explicit messages. TheHe also learned that few of Quon's on-duty messages were related to police business, and he was disciplined. Quon and other officers sued, alleging violations of the Fourth Amendment search and seizure provisions.

The trial court ruled that Quon and the police officers had an expectation of privacy in the content of the messages, but it dismissed the Fourth Amendment claims because the jury found that the police chief's actions were motivated by the legitimate reason of determining whether the officers were unfairly paying for work-related overages. The Ninth Circuit, however, reversed, concluding that the police chief's motives were not determinative because he could have used less intrusive tactics than an audit of the messages. The U.S. Supreme Court reversed, holding that the search of the text messages was not excessive in scope.

Kennedy, J.

***

Though the case touches issues of far-reaching significance, the Court concludes it can be resolved by settled principles determining when a search is reasonable.

***

It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *Camara v. Municipal Court of City and County of San Francisco*. "The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function. The Fourth Amendment applies as well when the Government acts in its capacity as an employer. *Treasury Employees v. Von Raab*.

***

Before turning to the reasonableness of the search, it is instructive to note the parties' disagreement over whether Quon had a reasonable expectation of privacy. The record does establish that OPD, at the outset, made it clear that pager messages were not considered private. The City's Computer Policy stated that "[u]sers should have no expectation of privacy or confidentiality when using" City computers. Chief Scharf's memo and Duke's statements made clear that this official policy extended to text messaging. The disagreement, at least as respondents see the case, is over whether Duke's later statements overrode the official policy. Respondents contend that because Duke told Quon that an audit would be unnecessary if Quon paid for the overage, Quon reasonably could expect that the contents of his messages would remain private.

At this point, were we to assume that inquiry into "operational realities" were called for, . . . it would be necessary to ask whether Duke's statements could be taken as announcing a change in OPD policy, and if so, whether he had, in fact or appearance, the authority to make such a change and to guarantee the privacy of text messaging. It would also be necessary to consider whether a review of messages sent on police pagers, particularly those sent while officers are on duty, might be justified for other reasons, including performance evaluations, litigation concerning the lawfulness of police actions, and perhaps compliance with state open records laws. These matters would all bear on the legitimacy of an employee's privacy expectation.

The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating

too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. See, e.g., *Olmstead v. United States,* overruled by *Katz v. United States*. In *Katz,* the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one amici brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another amicus points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

Even if the Court were certain that the O'Connor plurality's approach were the right one, the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.

A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds. For present purposes we assume several propositions arguendo: First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City; second, petitioners' review of the transcript constituted a search within the meaning of the Fourth Amendment; and third, the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.

Even if Quon had a reasonable expectation of privacy in his text messages, petitioners did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcripts. Although as a general matter, warrantless searches "are per se unreasonable under the Fourth Amendment," there are "a few specifically established and well-delineated exceptions" to that general rule . . . The Court has held that the "'special needs'" of the workplace justify one such exception.

Under the approach of the O'Connor plurality, when conducted for a "noninvestigatory, work-related purpos[e]" or for the "investigatio[n] of work-related misconduct," a government employer's warrantless search is reasonable if it is "'justified at its inception'" and if "'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of'" the circumstances giving rise to the search. The search here satisfied the standard of the O'Connor plurality and was reasonable under that approach.

The search was justified at its inception because there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose." As a jury found, Chief Scharf ordered the search in order to determine whether the character limit on the City's contract with Arch Wireless was sufficient to meet the City's needs. This was, as the Ninth Circuit noted, a "legitimate work-related rationale." The City and OPD had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand that the City was not paying for extensive personal communications.

As for the scope of the search, reviewing the transcripts was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use. The review was also not "'excessively intrusive.'" Although Quon had gone over his monthly allotment a number of times, OPD requested transcripts for only the months of August and September 2002. While it may have been reasonable as well for OPD to review transcripts of all the months in which Quon exceeded his allowance, it was certainly reasonable for OPD to review

messages for just two months in order to obtain a large enough sample to decide whether the character limits were efficacious. And it is worth noting that during his internal affairs investigation, McMahon redacted all messages Quon sent while off duty, a measure which reduced the intrusiveness of any further review of the transcripts.

Furthermore, and again on the assumption that Quon had a reasonable expectation of privacy in the contents of his messages, the extent of an expectation is relevant to assessing whether the search was too intrusive. Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing. As a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. Given that the City issued the pagers to Quon and other SWAT Team members in order to help them more quickly respond to crises—and given that Quon had received no assurances of privacy—Quon could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team's performance in particular emergency situations.

From OPD's perspective, the fact that Quon likely had only a limited privacy expectation, with boundaries that we need not here explore, lessened the risk that the review would intrude on highly private details of Quon's life. OPD's audit of messages on Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been. That the search did reveal intimate details of Quon's life does not make it unreasonable, for under the circumstances a reasonable employer would not expect that such a review would intrude on such matters. The search was permissible in its scope.

Case Questions

1. The Supreme Court and the Ninth Circuit reached different conclusions on the issue of the proper scope of the search. Which one do you think is the better approach? Why?
2. Both courts agreed that Quon did not have a reasonable expectation of privacy in the text messages, despite the fact that his boss told him that the messages would be private if he paid the overages. What statements or acts by an employee, in your opinion, would be necessary to create an expectation of privacy in the messages? Where is the line drawn?
3. Would this case, in your opinion, have been decided differently if it had involved an employer-supplied communication device other than a pager? If so, how?
4. Do you agree with the statement that an audit of text messages is less intrusive than a phone wiretap? Why or why not?
5. The Court decided the case on narrow grounds, purposefully stopping short of pronouncing broadly applicable rules for electronic communications. If they had taken on the task of a broadly applicable rule, what, in your opinion, should they have said?