Chapter 7
ETHICAL DECISION-MAKING:
TECHNOLOGY AND PRIVACY IN THE WORKPLACE
“People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people—and that social norm is just something that has evolved over time.”

Mark Zuckerberg, co-founder and CEO, Facebook

“Things do not change; we change.”

Henry David Thoreau
CHAPTER OBJECTIVES

After exploring this chapter, you will be able to:

1. Explain and distinguish the two definitions of privacy.
2. Describe the ethical sources of privacy as a fundamental value.
3. Identify the three legal sources of privacy protection.
4. Discuss the concept of a “reasonable expectation of privacy.”
5. Discuss recent development in connection with employee monitoring.
6. Explain the risks involved in a failure to understand the implications of technology and its use.
7. Identify additional ethical challenges posed by technology use.
8. Articulate the manner in which employee monitoring works.
CHAPTER OBJECTIVES

9. Enumerate the reasons why employers choose to monitor employees’ work.
10. Discuss the ethics of monitoring as it applies to drug testing.
11. Discuss the ethics of monitoring as it applies to polygraphs, genetic testing, and other forms of surveillance.
12. Explain why monitoring might also pose some costs for the employer and for the employee.
13. Discuss the elements of a monitoring program that might balance the interests of the employee and the employer.
14. Explain the interests of an employer in regulating an employee’s activities outside of work.
15. Discuss the implications of September 11, 2001, for privacy rights.
OPENING DECISION POINT: BEING SMART ABOUT SMARTPHONES

- Is it unethical to use your smartphone during a meeting? Why do you think someone else might give a different answer than you do?

- Would your answer be different if the person in question was using a smartphone to communicate with another client during a meeting, rather than taking notes?

- Is it anyone else’s business what you’re doing on your phone during a meeting? In other words, do you have a privacy right to do whatever you want on your phone?

- As a practical matter, how might misunderstandings about smartphone use be avoided?
OPENING DECISION POINT: BEING SMART ABOUT SMARTPHONES

- In what ways have smartphones probably changed the way we do business? How have they changed the way people interact with each other in the workplace?
- What is the connection, if any, between manners and ethics? If use of a smartphone during a meeting is considered rude by some people, at what point if any does rudeness become unethical?
THE RIGHT TO PRIVACY

- 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 rights have increased.
- There is widespread confusion concerning the nature, extent, and value of privacy.
DEFINING PRIVACY

- Two general and connected understandings of privacy:
  - Privacy as a *right to be* “left alone” within a personal zone of solitude
  - Privacy as the *right to control information* about oneself
THE VALUE OF PRIVACY

- Privacy serves to establish the boundary between individuals and thereby serves to define one’s individuality.
- The right to control certain extremely personal decisions and information helps determine the kind of person we are and the person we become.
- To the degree that we value the inherent dignity of each individual and the right of each person to be treated with respect, we must recognize that certain personal decisions and information are rightfully the exclusive domain of the individual.
WHAT IS PRIVACY

- An individual's privacy is violated or not by a disclosure of personal information depends upon the relationship between the individual and with the person or persons who come to know that information.
- Limiting access of personal information to only those with whom one has a personal relationship is one important way to preserve one’s own personal integrity and individuality.
- It is the *choice of limitation* or *control* that is the source of one’s sense of privacy.
The right to privacy is founded in the individual’s fundamental, universal right to autonomy, in our right to make decisions about our personal existence without restriction.

This right is restricted by a social contract in our culture that prevents us from infringing on someone else’s right to her or his personal autonomy.

**Reciprocal obligation**: For an individual to expect respect for her or his personal autonomy, that individual has a reciprocal obligation to respect the autonomy of others.
Applied to the workplace, the concept of reciprocal obligation implies that, while an employee has an obligation to respect the goals and property of the employer, the employer has a reciprocal obligation to respect the rights of the employee as well, including the employee’s right to privacy.

Ethicists Thomas Donaldson and Thomas Dunfee have developed an approach to ethical analysis that seeks to differentiate between those values that are fundamental across culture and theory hypernorms and those values that are determined within moral free space and that are not hypernorms.
ETHICAL SOURCES OF A RIGHT TO PRIVACY

- Donaldson and Dunfee propose that we look to the convergence of religious, cultural, and philosophical beliefs around certain core principles as a clue to the identification of hypernorms.

- Donaldson and Dunfee include the following as examples of hypernorms:
  - Freedom of speech
  - The right to personal freedom
  - The right to physical movement
  - Informed consent

- Individual privacy is at the core of many of these basic minimal rights and a necessary prerequisite to many of them.
ETHICAL SOURCES OF A RIGHT TO PRIVACY

- The value of privacy to civilized society is as great as the value of the various hypernorms to civilized existence.
- The failure to protect privacy may lead to an inability to protect personal freedom and autonomy.
PROPERTY RIGHTS

- “Property” is an individual’s life and all non-procreative derivatives of her or his life.
  - Derivatives include thoughts, ideas, and personal information.
- The concept of property rights involves a determination of who maintains control over tangibles and intangibles, including personal information.
- Property rights relating to personal information define actions that individuals can take in relation to other individuals regarding their personal information.
  - If one individual has a right to her or his personal information, someone else has a commensurate duty to observe that right.
PROPERTY RIGHTS

- Private property rights depend upon the existence and enforcement of a set of rules that define:
  - Who has a right to undertake which activities on their own initiative.
  - How the returns from those activities will be allocated.
Privacy can be legally protected in three ways:

- By the constitution (federal or state)
- By federal and/or state statutes
- By the common law
  - **Common law**: Body of law comprised of the decisions handed down by courts, rather than specified in any particular statutes or regulations.

The Constitution’s **Fourth Amendment protection against an unreasonable** search and seizure governs only the public sector workplace because the Constitution applies only to state action.

- Unless the employer is the government or other representative of the state, the Constitution generally will not apply.
The Electronic Communications Privacy Act of 1986 (ECPA) prohibits the “interception” or unauthorized access of stored communications.

- Courts have ruled that “interception” applies only to messages in transit and not to messages that have actually reached company computers.
  - The impact of the ECPA is to punish electronic monitoring only by third parties and not by employers.
- The ECPA allows interception where consent has been granted.
  - A firm that secures employee consent to monitoring at the time of hire is immune from ECPA liability.
The “invasion of privacy” claim with which most people are familiar is one that developed through case law called intrusion into seclusion. This legal violation occurs when someone intentionally intrudes on the private affairs of another when the intrusion would be “highly offensive to a reasonable person.”

As we begin to live more closely with technology, and the intrusions it allows, we begin to accept more and more intrusions in our lives as reasonable.

As privacy invasions become more common, they begin to be closer to what is normal and expected.

It may no longer be reasonable to be offended by intrusions into one’s private life that used to be considered unacceptable.
Most recent court decisions with regard to monitoring specifically seem to depend on whether the worker had notice that the monitoring might occur.

Since the basis for finding an invasion of privacy is often the employee’s legitimate and reasonable expectation of privacy, if an employee has actual notice, then there truly is no real expectation of privacy.
| **Telephone calls** | Monitoring is permitted in connection with quality control. Notice to the parties on 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, it’s right to monitor has been upheld. However, where the employee’s reasonable expectation of privacy is increased (such as a password-protected account), this may impact the court’s decision. |
| **Voice-mail system messages** | Though not yet completely settled, the law here appears to be similar to the analysis of e-mail messages. |
| **Internet use** | Where the employer has provided the equipment and/or access to the Internet, the employer may track, block, or review Internet use. |
Global Applications

- Unpredictable regime of privacy protection is all the more problematic to maintain when one considers the implications of the European Union’s Directive on Personal Data Protection.

- The directive strives to harmonize all the various means of protecting *personal data* throughout the European Union, where each country originally maintained myriad standards for information gathering and protection.

- The directive prohibits E.U. firms from transferring personal information to a non-E.U. country unless that country maintains “adequate protections” of its own.
Because the United States would not qualify as having adequate protection, the U.S. Department of Commerce negotiated a Safe Harbor exception for firms that maintain a certain level of protection of information.

Considering the nature of the legal uncertainty or instability concerning these challenging areas of information gathering, the only source of an answer is ethics.
EMPLOYEE PRIVACY

- If we adopt something like a contractual model of employment—where the conditions and terms of employment are subject to the mutual and informed consent of both parties—then employee consent would become one major condition on what information employers can collect.

- Employee privacy is violated whenever:
  - Employers infringe upon personal decisions that are not relevant to the employment contract.
  - Personal information that is not relevant to that contract is collected, stored, or used without the informed consent of the employee.
The Safe Harbor exception requires that the receiving firm provide the following:

- Clear and conspicuous notice about the personal information collected.
- Choice to opt out of information collection or dissemination.
- Transfer of information to other firms only if they also demonstrate that they maintain the same level of adequate protections.
- Reasonable measures to ensure reliability of the information and protection from disclosure or loss of the information.
- Limitation to information that is relevant to the purpose for which it was gathered; that is, the firm does not access any information that is unrelated to its purposes.
- Access by the subject of the information, who then has the ability to correct any misinformation.
- Mechanisms for ensuring compliance and consequences for noncompliance.
Consider the implications of new technology on:

- Employee and employer expectations regarding the use of time.
- The distinction between work use and personal use of technology.
- The protection of proprietary information, performance measurement.
- Privacy interests; or accessibility issues related to the digital divide.

Technology allows for in-home offices, raising extraordinary opportunities and challenges, issues of safety, and privacy concerns.

Technology allows employers to ask more of each employee.

New technology does not impact our value judgments but instead simply provides new ways to gather the information on which to base them.
Firms experience, and find themselves ill prepared for, unanticipated challenges stemming from new technology.

Do we need “new ethics” for this “new economy?”

- The same values one held under previous circumstances should, if they are true and justified, permeate and relate to later circumstances.
- The perspective one brings to each experience is impacted by the understanding and use of new technology and other advances.
INFORMATION AND PRIVACY: GOOGLE’S EXPERIENCE

- A business needs to be able to anticipate the perceptions of its stakeholders in order to be able to make the most effective decisions for its long-term sustainability.
- New technological advancements are often difficult for the public to understand and therefore ripe for challenge.
- The motto at Google is the deontological imperative: “don’t be evil.”
- Google believed it was providing a value to society when it created Gmail.
  - Yet, critics charged that Google violated its own principles when it developed Gmail.
WHOM CAN YOU TRUST?

- Trust is truly the crux of the issue with the introduction of new technology.
- When consumers rely on technology provided by a business—from email to internet access and from cell phones to medical labs—they might easily assume that the business will respect their privacy.
- Most average email users do not understand the technology behind the process.
- One would like to believe that those responsible for the technology are, themselves, accountable to the user.
  - That would be the ideal.
EPIC SAYS: NOT GOOGLE

- The Electronic Privacy Information Center, a consumer advocacy group, considered Google’s marketing plan to be equivalent to a telephone operator who listens in on conversations and then pitches advertisements where relevant.
- The scanning device violated the two fundamental elements of privacy:
  - The right to be left alone.
  - The right to control information about oneself.
- Since the scanning and targeting of ads took place without the user’s original knowledge or consent, it violated the autonomy in the user’s right to make decisions about her or his “personal existence.”
- If one’s personal information is respected as property, Google used individual property without consent.
GOOGLE’S RESPONSE

- Google said that they were not doing anything more than the other services (who also include advertisements) except that its advertisements was more relevant to the user’s interests.
- In fact, their research showed that people actually followed many of those advertisements and ultimately made purchases.
By failing to fully comprehend and plan for its stakeholders’ perceptions of the program, Google not only breached ethical boundaries but also suffered public backlash. Critics argued that Google should have consulted with stakeholders, determined the best way to balance their interests, and then considered these interests as they introduced the new program, all of which might have precluded the negative impact on its reputation. The lesson learned is that, notwithstanding even reasonable justification people are simply not comfortable with an involuntary loss of control over these personal decisions. Google failed to consider the perspectives of its stakeholders, the impact of its decisions on those stakeholders, and the fundamental values its decision implied.
RECOMMENDED MORAL REQUIREMENTS

- Economist Antonio Argandona contends that, if new technology is dependent on and has as its substance information and data, following elements are necessary:
  - Truthfulness and accuracy
  - Respect for privacy
  - Respect for property and safety rights
  - Accountability
One of the most prevalent forms of information gathering in the workplace, in particular, is monitoring employees’ work, and technology has afforded employers enormous abilities to do so effectively at very low costs.

The American Management Association has conducted surveys of mid- to large-sized U.S. firms over the past few years that show an increasing trend with regard to employee e-mail monitoring.
MANAGING EMPLOYEES THROUGH MONITORING

- According to one study, about half of companies have engaged in surveillance of employee email.
- Another survey found that only 10% of companies monitor employee use of Facebook, YouTube, LinkedIn, etc., but 60% of companies said they anticipated doing so by 2015.
RISKS INVOLVED IN FAILURE TO UNDERSTAND TECHNOLOGY

- Many of the ethical issues that arise in the area of managing information are not readily visible.

- When we do not understand technology, we are not able effectively to protect our own information because we may not understand:
  - The impact on our autonomy
  - The control of our information
  - Our reciprocal obligations
  - What might be best for our personal existence.
RISKS INVOLVED IN FAILURE TO UNDERSTAND TECHNOLOGY

- Ethical issues may be compounded by the fact that a knowledge gap exists between people who do understand the technology and others who are unable to protect themselves precisely because they do not understand.
ETHICAL CHALLENGES POSED BY TECHNOLOGY USE

- Technology allows for access to information that was never before possible.
- Access can take place unintentionally.
  - In doing a routine background check, a supervisor may unintentionally uncover information of an extremely personal nature that may bear absolutely no relevance to one’s work performance.
- This occurs because the information, though previously unavailable or too burdensome to uncover, is now freely available from a variety of sources.
CONTINUOUS ACCESSIBILITY BLURS THE LINES BETWEEN OUR PERSONAL AND PROFESSIONAL LIVES!

- Technology allows us to work from almost anywhere on this planet, we are seldom out of the boundaries of our workplace.
- This raises a tough question: should your supervisor try to reach you just because she has the ability?
  - Our total accessibility creates new expectations, and therefore conflicts.
FACELESSNESS MAY BREED CARELESSNESS

- When we do not get to know someone because we do not have to see that person in order to do our business, we do not take into account the impact of our decisions on that person.

- They become merely a name at the other end of an email correspondence, rather than another human being.

- Given the ease and informality of electronic communications, we “say” (write, e-mail, and the like) things to each other that we would never say to someone’s face
  - Because we do not have to consider the impact of what we are saying.

- We are more careless with our communications because they are easier to conduct—just hit a button and they are sent.
WHY DO FIRMS MONITOR TECHNOLOGY USAGE?

- Employers need to manage their workplaces to place workers in appropriate positions.
- To ensure compliance with affirmative action requirements.
- To administer workplace benefits.
- Monitoring allows the manager to ensure effective, productive performance by preventing the loss of productivity to inappropriate technology use.
- Monitoring offers an employer a method by which to protect its others resources.
  - Employers use monitoring to protect proprietary information and to guard against theft, to protect their investment in equipment and bandwidth, and to protect against legal liability.
With regard to drug or other substance testing, the employer has a strong argument in favor of testing based on the law.

Since the employer is often responsible for legal violations of its employees committed in the course of their job, the employer's interest in retaining control over every aspect of the work environment increases.

Employees may argue that their drug usage is only relevant if it impacts their job performance.

Until it does, the employer should have no basis for testing.
In the seminal legal case on the issue, Skinner v. Railway Labor Executives’ Ass’n, the Court addressed the question of whether certain forms of drug and alcohol testing violate the Fourth Amendment.

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.”
LEGALITY OF DRUG TESTING

- The court held that “the 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, absent a warrant or individualized suspicion, the means by which the defendant monitored compliance with this prohibition justified the privacy intrusion.

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."

The court 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.”
LEGALITY OF DRUG TESTING

- The court therefore concluded that the railway’s compelling interests outweighed privacy concerns since the proposed testing “is not an undue infringement on the justifiable expectations of privacy of covered employees.”
- The railway was allowed to test employees.
ETHICS OF DRUG TESTING

- Where public safety is at risk, there is arguably a compelling public interest claim from a utilitarian perspective that may be sufficiently persuasive to outweigh any one individual’s right to privacy or right to control information about oneself.

- However, what about jobs in which public safety is not at risk? Is it justifiable to test all employees and job applicants?

- Is the proposed benefit to the employer sufficiently valuable in your perspective to outweigh the employee’s fundamental interest in autonomy and privacy?
ETHICS OF DRUG TESTING

- Should a utilitarian viewpoint govern or should deontological principles take priority?
- Should we consider a distributive justice perspective and the fairest result—does distributive justice apply under these circumstances?
OTHER FORMS OF MONITORING

- Employers are limited in their collection of information through other various forms of testing, such as polygraphs or medical tests.
- 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).

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.
THE FUTURE OF TESTING

- In recent years polygraph and drug testing, physical and electronic surveillance, third-party background checks, and psychological testing have all been used as means to gain information about employees.
- Electronic monitoring and surveillance are increasingly being used in the workplace.
- In future, genetic testing will raise new questions about privacy.
  - Genetic testing and screening, of both employees and consumers, is another new technology that will offer businesses a wealth of information about potential employees and customers.
- The Genetic Information Non-Discrimination Act of 2008 (GINA) became effective in November 2009 and prohibits discriminatory treatment in employment based on genetic information.
GINA

- It defines “genetic information” in a more broad sense.
- Under GINA, your genetic information is not merely information about you, but also your family’s medical history, including any disease or disorder, or genetic test results of a family member.
- GINA mandates that employers be extremely careful in terms of how they gather and manage employee genetic information as they are subject to similar conditions to the Americans with Disabilities Act.
GINA

- GINA does provide for exceptions.
  - An employer can collect genetic information in order to comply with the Family Medical Leave Act or to monitor the biological effects of toxic substances in the workplace.
  - The employer may also gather publicly available genetic information, from public sources such as newspapers.
  - Though GINA contains a strict confidentiality provision, an employer may release genetic information about an employee under certain specific circumstances.
BUSINESS REASONS TO LIMIT MONITORING

- Monitoring may create a suspicious and hostile workplace.
- Monitoring may arguably constrain effective performance since it can cause increased stress and pressure, negatively impacting performance and having the potential to cause physical disorders such as carpal tunnel syndrome.
BUSINESS REASONS TO LIMIT MONITORING

- Stress might also result from a situation where workers do not have the opportunity to review and correct misinformation in the data collected.
  - These elements will lead to an unhappy, disgruntled worker who perhaps will seek alternative employment but to lower productivity and performance that will reap higher costs and fewer returns to the employer.
- Employees claim that monitoring is an inherent invasion of privacy in violation of their fundamental human right to privacy.
BALANCING INTERESTS

- It is suggested that due notice should be given to the employees, that they will be monitored.
- The opportunity to avoid monitoring in certain situations would solve the ethical problems.
- But such an approach may not solve all the concerns about monitoring.
- Effect of employer monitoring is termed the “Hawthorne Effect”
  - Workers are found to be more productive based on the psychological stimulus of being singled out, which makes them feel more important.
- Random, anonymous monitoring may be a better option.
BALANCING INTERESTS

- The most effective means to achieve monitoring objectives:
  - Remaining sensitive to the concerns of employees
  - Striving towards a balance that respects individual dignity while holding individuals accountable for their particular roles in the organization.
In 1997, the International Labour Organization published a Code of Practice on the Protection of Workers’ Personal Data, and it remains in use today. Though not binding on employers, it serves to help codify ethical standards in connection with the collection and use of employee personal information. The code includes, among others, the following principles:

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

5.4 Personal data . . . should not be used to control the behavior of workers.

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.

6.5 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.
The regulation of an employee’s activities when she or he is away from work is an interesting issue, particularly in at-will environments.

But, even employers of at-will employees must comply with a variety of statutes in imposing requirements and managing employees.
Across the nation, there are other less broad protections for off-work acts. A number of states have enacted protections about the consumption or use of legal products off the job, such as cigarettes. 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 anti-retaliation provisions for employers who violate the prohibition).
Employers are not prohibited from making employment decisions on the basis of weight, as long as they are not in violation of the American with Disabilities Act (ADA) when they do so. The issue depends on whether the employee’s weight is evidence of or results from a disability. If so, the employer must explore whether the worker is otherwise qualified for the position.
REGULATION OF OFF WORK ACTS: WEIGHT ISSUES

- Under the ADA, the individual is considered “otherwise qualified” if she or he can perform the essential functions of the position with or without reasonable accommodations.

- If the individual cannot perform the essential functions of the position, the employer is not subject to liability for reaching an adverse employment decision.

- Employers should be cautious 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 his or her weight.
Laws that protect against discrimination based on marital status exist in just under half of the states.

Though a worker might be protected based on marital status, they are not necessarily protected against adverse action based on the identity of the person they married.

Some companies might have an anti-nepotism policy where an employer refuses to hire or terminates a worker based on the spouse working at the same firm, or a conflict-of-interest policy where the employer refuses to hire or terminates a worker whose spouse works at a competing firm.
Since about 40% of workers have dated an office colleague, policies and attitudes on workplace dating are especially significant.

Though only about 13 percent of workplaces have policies addressing workplace dating, a New York decision reaffirms the employer’s right to terminate a worker on the basis of romantic involvement.
REGULATION OF OFF WORK ACTS: POLITICAL INVOLVEMENT

- The majority of states protect against discrimination on the basis of political involvement, though states vary on the type and extent of protection.
- Lifestyle discrimination may be unlawful if the imposition of the rule treats one protected group differently than another.
- Similarly, the rule may be unlawful if it has a different impact on a protected group than on other groups.
Most statutes or common law decisions provide for employer defenses for those rules that:

- Are reasonably and rationally related to the employment activities of a particular employee.
- Constitute a “bona fide occupational requirement,” meaning a rule that is reasonably related to that particular position.
- Are necessary to avoid a conflict of interest or the appearance of conflict of interest.
The question of monitoring and managing employee online communications while the employee is off work emerges as an astonishingly challenging area of conflict between employers and employees, and one without much legal guidance, demanding sensitive ethical decision making.

While employers are legally prevented from asking candidates about their religion or prior illegal drug use during a job interview, is it ethical for them to seek out that information through online sources when the candidate voluntarily discloses it with no connection with work?
The events of September 11, 2001 have had major impacts on privacy within the United States, and with the employment environment in particular. The federal government has implemented widespread modifications to its patchwork structure of privacy protections since the terror attacks of September 11, 2001. Proposals for the expansion of surveillance and information gathering authority were submitted and, to the chagrin of some civil rights attorneys and advocates, many were enacted.
The most public and publicized of the modifications was the adoption and implementation of the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism United States (USA PATRIOT) Act of 2001**.

The USA PATRIOT Act expanded States’ rights with regard to Internet surveillance technology, including workplace surveillance and amending the Electronic Communications Privacy Act.
USA PATRIOT ACT

- The Act also grants access to sensitive data with only a court order rather than a judicial warrant 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.
THE ACT’S IMPACT ON EMPLOYERS’ EFFORTS TO MAINTAIN EMPLOYEE PRIVACY

- The Act provides for the following enhanced procedures:
  - Expanded authority to intercept wire, oral, and electronic communications relating to terrorism and to computer fraud and abuse offenses.
  - Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978 (FISA) to track individuals.
  - Nationwide seizure of voice-mail messages pursuant to warrants (i.e. without the previously required wiretap order).
  - Broadens the types of records that law enforcement may obtain, pursuant to a subpoena, from electronic communications service providers.
  - Permits emergency disclosure of customer electronic communications by providers to protect life and limb.
  - Nationwide service of search warrants for electronic evidence.
Employers have three choices in terms of their response to a governmental request for information.

- They may opt to voluntarily cooperate with law enforcement by providing confidential employee or customer information upon request and as part of an ongoing investigation.
- They may choose to cooperate by asking for permission to seek employee authorization to release the requested information.
- They may request to receive a subpoena, search warrant, or FISA order from the federal agency before disclosing an employee’s confidential information.
OPENING DECISION POINT REVISITED:
BEING SMART ABOUT SMARTPHONES

- Try putting yourself in the shoes of the CFO who was offended by the smartphone use during the meeting. What legitimate concerns might she have about the way the meeting went? What specifically might she be worried about?

- Would it make any difference if the electronic device involved was something other than a smart phone – say, a laptop or an iPad or other tablet computer?
There may well be a generation gap that explains different reactions to the use of smartphones during a business meeting. How deep is that gap? Have people’s values changed, or just the way they demonstrate those values?
CHAPTER SEVEN VOCABULARY TERMS

After examining this Chapter, you should have a clear understanding of the following Key Terms and you will find them defined in the Glossary:

- Electronic Communications Privacy Act of 1986
- e-mail monitoring
- European Union’s Directive on Personal Data Protection
- Fourth Amendment protection
- HIPAA
- hypernorms
- Internet use monitoring
- Intrusion into seclusion
- Moral free space
CHAPTER SEVEN VOCABULARY TERMS

- Personal data
- Privacy
- Privacy rights
- Property rights perspective
- Reasonable expectation of privacy
- Reciprocal obligation
- Safe Harbor exception
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001