CHAPTER 8
Ethics and Technology

Chapter Summary

This chapter examines the ethical debate over employee surveillance and the extent to which technology not only facilitates the prevention of unethical behavior but also jeopardizes the rights of individual employees. The chapter begins by displaying the types of new technology and the ethical implications of using it. Further, the chapter discusses the different points of view on privacy at work from an employer and an employee perspective. Finally, the chapter discusses the privacy and surveillance capabilities and the future of surveillance used in corporations.

Learning Objectives

After studying this chapter, the student should be able to:

1. Evaluation the ethical ramifications of recent technological advances.
2. Explain the employer view of privacy at work.
3. Explain the employee view of privacy at work.
4. Distinguish between thin and thick consent.
5. Evaluate the concept of vicarious liability.
6. Analyze an organization’s employee-surveillance capabilities.
7. Discuss the future of corporate surveillance for employees.

Extended Chapter Outline

Objective 1: Evaluation the ethical ramifications of recent technological advances.

1.1. The opening Frontline Focus case shows how an employee faces an ethical decision with a co worker.

1.2. Advantages of technology in the workplace.
   1.2.1. Internet
   1.2.2. Intranet is a company’s internal website, containing information for employee access only.
   1.2.3. Extranet is a private piece of a company’s internet network that is made available to customers and/or vendor partners on the basis of secured access by unique password.

1.3. Disadvantages of technology in the workplace include the loss of privacy in two key areas:
   1.3.1. Customers must be aware that companies now have the technical capability to send their personal data to any part of the world to take advantage of lower labor costs.
   1.3.2. Employees must be aware that employers now have capability of monitoring every email you send and web site you visit in order to make...
sure that you really are delivering on the promise of increased worker productivity.

Objective 2: Explain the employer view of privacy at work.
2.1. Productivity in the workplace is what the employees have to meet for the pay-for-performance contract they agreed to when they were hired.
   2.1.1. Your actions during work time are at the discretion of the company.
2.2. Company has obligation to its stakeholders to run efficiently and ensure resources are not misused and information is closely guarded.

Objective 3: Explain the employee view of privacy at work.
3.1. As an employee the time at work represents the productivity for which I get compensation in return.
3.2. Employee not a servant
   3.2.1. The compensation agreement should not allow the employer to intrude the employees’ civil rights as an individual.
   3.2.2. Electric monitoring implies that employees’ can’t be trusted to do their jobs

Objective 4: Distinguish between thin and thick consent.
4.1. Telecommuting: The ability to work outside the office (from your home or anywhere else) and log into your company network (usually via a secure gateway such as a VPN, virtual private network).
4.2. Thick Consent: When jobs are plentiful and the employee would have no difficulty in finding another position, then the employee has a realistic alternative if he or she finds a monitoring policy unacceptable, and consent can be classified as thick.
4.3. Thin Consent: When an employee receives formal notification that the company will be monitoring all email and Web activity. Either at the time of hire or during employment and is made clear in that notifications that his or her continued employment with the company will be dependent on the employee’s agreement to abide by that monitoring.

Objective 5: Evaluate the concept of vicarious liability.
5.1. Vicarious Liability: A legal concept that means a party may be held responsible for injury or damage even when he or she was not actively involved in the incident.
5.2. Cyberliability: Employers can be held liable for the actions of their employees in their internet communications to the same degree as if those employers had written those communications on company letterhead.
   5.2.1. The extent of this new liability can be seen in the top categories of litigation recorded by Elron Software:
      5.2.1.1. Discrimination
      5.2.1.2. Harassment
      5.2.1.2.1. Obscenity and pornography
      5.2.1.2.2. Defamation and libel
Objective 6: Analyze an organization’s employee-surveillance capabilities.

6.1. An employer has the capabilities to surveillance every keystroke on your computer, track every website you visit, and record every call you make.
   6.1.1. Creating this type of environment may protect your liability, but may drive those employees away who are less comfortable with this method.

6.2. Ten Commandments of Computer Ethics
   6.2.1. Thou shall not use a computer to harm other people
   6.2.2. Thou shall not interfere with other people’s computer work
   6.2.3. Thou shall not snoop around in other people’s computer files
   6.2.4. Thou shall not use a computer to steal
   6.2.5. Thou shall not use a computer to bear false witness
   6.2.6. Thou shall not copy or use proprietary software for which you have not paid
   6.2.7. Thou shall not use of people’s computer resources without authorization or proper compensation
   6.2.8. Thou shall not appropriate other people’s intellectual output.
   6.2.9. Thou shall not think about the social consequences of the program you are writing or the system you are designing
   6.2.10. Thou shall not always use a computer in ways that ensure consideration and respect for your fellow humans.

Objective 7: Discuss the future of corporate surveillance for employees.

7.1. Demands of a techno-friendly school of ethics is likely to continue

7.2. Due to the availability of instant access at the work place means the line between work life and private life is much less clearly defined.
   7.2.1. This change should mean that the employer’s ability to intrude on our personal lives with an urgent request would be balanced by an equal flexibility in our time at work.

7.3. Invasive tools that exist to monitor employees at the workplace:
   7.3.1. Packet-sniffing software can intercept, analyze and archive all communications on a network, including employee email, chat sessions, file sharing and internet browsing.
   7.3.2. Keystroke loggers can be employed to capture every key pressed on a computer keyboard.
   7.3.3. Place monitoring is pervasive in the American workplace
   7.3.4. Video surveillance is widely developed in the American workplace
   7.3.5. “Smart” ID cards can track an employee’s location while he or she moves throughout the workplace
Key Terms

**Cyberliability:** Employers can be held liable for the actions of their employees in their internet communications to the same degree as if those employers had written those communications on company letterhead.

**Thick Consent:** When jobs are plentiful and the employee would have no difficulty in finding another position, then the employee has a realistic alternative if he or she finds a monitoring policy unacceptable, and consent can be classified as thick.

**Extranet:** A private piece of a company’s internet network that is made available to customers and/or vendor partners on the basis of secured access by unique password.

**Thin Consent:** When an employee receives formal notification that the company will be monitoring all email and Web activity. Either at the time of hire or during employment and is made clear in that notifications that his or her continued employment with the company will be dependent on the employee’s agreement to abide by that monitoring.

**Intranet:** A company’s internal website, containing information for employee access only.

**Vicarious Liability:** A legal concept that means a party may be held responsible for injury or damage even when he or she was not actively involved in the incident.

**Telecommuting:** The ability to work outside the office (from your home or anywhere else) and log into your company network (usually via a secure gateway such as a VPN, virtual private network).