

Information Management and Society

Chapter Outline

- Introduction, 917
- Individuals, 918
 - Privacy, 919*
 - Privacy Laws and Rules, 930*
 - Anonymity, 931*
- Jobs, 932
 - Loss of Jobs, 932*
 - Physical Disabilities, 934*
 - Telecommuting, 934*
- Business: Vendors and Consumers, 936
 - Intellectual Property, 936*
 - Digital Rights Management, 940*
 - Balance of Power, 942*
- Education and Training, 944
- Social Interactions, 945
 - Social Group Legitimacy, 945*
 - Access to Technology, 948*
 - e-Mail Freedom, 949*
 - Liability and Control of Data, 949*
- Government, 950
 - Government Representatives and Agencies, 950*
 - Democracy and Participation, 950*
 - Voting, 951*
 - Information Warfare, 953*
 - Rise of the World-State?, 955*
 - World Government Cases, 956*
- Crime, 959
 - Police Powers, 959*
 - Freedom of Speech, 960*
 - Gambling, 961*
- Responsibility and Ethics, 962
 - Users, 962*
 - Programmers and Developers, 963*
 - Companies, 964*
 - Governments, 964*
- Some Computer-Related Laws, 965
 - Property Rights, 965*
 - Privacy, 968*
 - Information Era Crimes, 971*
- Cloud Computing, 972
 - Data in Multiple Countries, 973*
 - Threats to Shared Servers, 974*
 - Subcontractors, 975*
- Summary, 976
- Key Words, 977
- Web Site References, 978
- Review Questions, 978
- Exercises, 979
- Additional Reading, 982
- Cases: Health Care, 983

What You Will Learn in This Chapter

- How does your company affect the rest of the world? What influence does the outside world have on your company?
- How does information technology affect individuals? As a manager and a company, do you treat individuals the way you expect to be treated by other companies?
- How does technology affect jobs? If computers do more of the work, what jobs are left for people?
- How does technology change the relationship between businesses and consumers?
- Can information technology change education?
- How does technology affect different areas of society?
- Can information technology improve governments?
- Do criminals know how to use computers?
- How do your actions affect society? Is it possible to follow the laws and still be wrong?
- What major laws affect technology and the use of computers?
- What risks are created through using cloud computing?

Sutter Health

How do information systems affect society? From one perspective, health care organizations are simply another business. Yet, because of their costs, importance to our daily lives, and widespread governmental involvement, health care has a special role in society. Not surprisingly, most physicians and other health care workers receive minimal training in information systems and are not comfortable with it. Consequently, information systems for medical care are being introduced slowly. On the other hand, information systems have the ability to reduce errors as well as costs. In particular, health care organizations like Sutter Health are working to implement electronic drug ordering and dispensing systems. Sutter is also working to implement paperless medical offices and already has 400 member physicians using a completely electronic system—including X-rays and prescriptions. The group is also working with telemedicine—particularly with intensive care units (ICUs) to reduce the costs of physicians and provide better care to remote locations. Of course, security and privacy issues become major areas of concern with medical information systems.

Introduction

How does your company affect the rest of the world? What influence does the outside world have on your company? Why should you care? Try an easier question: How much do your customers care about privacy? When you use information technology to help your company, it means you are collecting and analyzing data on customers and employees. As shown in Figure 14.1, your company lives within an environment. Companies influence the world through relationships with customers, employees, and other companies. In turn, your organization is affected by events in the world ranging from government laws to education and public opinion. When you make business decisions, you need to think about these interaction effects. Even if you cannot change the world yourself, you should be aware of the effects of your choices so that you are ready to deal with the consequences.

If nothing else, history has shown that technological change is inevitable. Competitive economics virtually guarantees that the search for new products, new manufacturing techniques, and other ways to gain competitive advantage will continue. Changes in technology often affect society. Technology can change individuals, jobs, education, governments, and social interactions. As components of society, each group has rights and responsibilities to others, such as a right to privacy and obligations regarding ethics.

Technology effects on individuals can be beneficial or detrimental. Often a change in technology helps one set of individuals and harms another group. Typical problems include loss of privacy, depersonalization, and changing incentives or motivations. Advantages include lower prices and better products and service. The effect on jobs is hard to predict, but most observers conclude that workers will require more education and training. Most authorities think that increases in technology in the past generally led to an increase in the number of jobs. Now, however, many of the new jobs require higher levels of education, and the workers displaced by technology rarely have the qualifications needed for the new jobs.

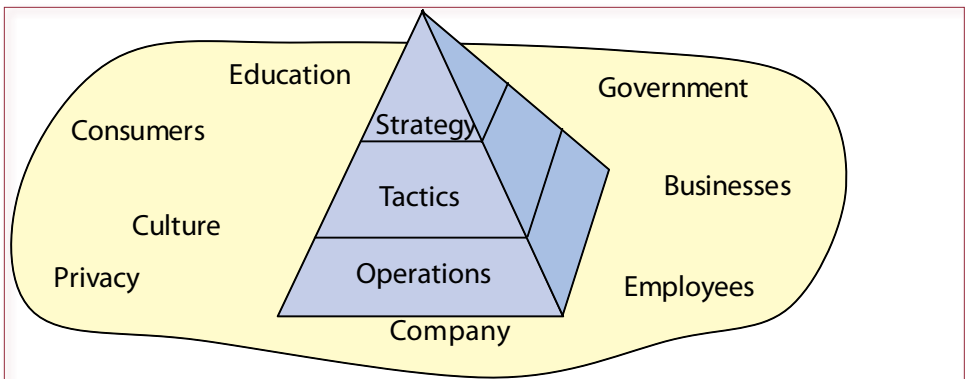


Figure 14.1

Information management and society. Every organization and individual exist in a social environment. Changes in the firm and changes in technology affect the environment. Changes in the environment can affect the firm. An understanding of these interactions will make you a better manager.

Technology also has an effect on crime. Technology creates new crimes, new ways to commit crimes, and new ways to catch criminals.

In addition to the increased demand, technology has provided new teaching methods. Although there is considerable debate over the costs and benefits of technology in education, there is usually a place for technology, even if only as a specialized technique. However, most educators know that technology cannot succeed by itself. Technology can isolate or it can build connections, but it requires people and applications to improve learning.

Governments attempt to control these impacts of technology by creating laws, but laws often bring their own problems. Also, in times of rapid change, laws rarely keep up with the changes in technology. Governments are also directly affected by improved communication facilities. For example, technology makes it possible for governments to better understand the needs of the citizens and provide more avenues for communication.

Technology can alter any number of social interactions. Social groups can gain or lose power, and types or methods of criminals are altered. Furthermore, society can become dependent on technology, which is not necessarily bad, but it causes problems if the technology is removed or substantially altered.

Individuals

How does information technology affect individuals? As a manager and a company, do you treat individuals the way you expect to be treated by other companies? Information technology plays an important role in the lives of most individuals. Many jobs are directly involved in the collection, processing, and evaluation of data. Performance of many workers is continually monitored by computers. As consumers, virtually our entire lives are recorded and analyzed. Governments maintain massive files on all public aspects of our lives. Increasingly, these public files are accessible to anyone via the Web and a few dollars. **Privacy** is a delicate and controversial issue. Citizens must work together to live in a society, which requires giving up some elements of pri-

Trends

The industrial revolution in the late 18th century caused many changes to society. Before the revolution, workers were predominantly employed as craftsmen, farmers, or lesser-skilled laborers. Mechanization brought standardization and assembly lines, for which jobs were reduced to simple, repetitive tasks.

As transportation improved, people moved from farms to cities, and cities spread to suburbs. Communication systems improved and linked the populations back together. Better product distribution mechanisms changed the way products are sold. Companies (such as Sears, through its catalogs) began to distribute products nationally instead of relying on small local stores. National and international markets developed with every change in the communication and transportation systems.

These changes were so strong that philosophers and writers began to take note of how technological changes can affect society. From the bleak pictures painted by Dickens, Marx, and Orwell, to the fantastic voyages of Verne, Heinlein, and Asimov, we can read thousands of opinions and predictions about how technology might affect the political, economic, and social environments.

vacuity. Businesses and governments often need to identify customers and employees to perform basic functions. Yet history reveals that individuals can be threatened or coerced if some people or organizations collect too much information.

Although data has been collected on citizens for many years, recent improvements in technology raise greater concerns about privacy. As computer capabilities increase, it becomes possible to collect, integrate, and analyze the huge volume of data. Using publicly available data, it is possible to collect an amazing amount of data on any person.

Privacy

As Figure 14.2 indicates, companies, governments, and employers collect data about many aspects of our lives. Most of the modern marketing efforts including data mining and building customer relationships require information about customers. Marketing and sales can be improved by maintaining databases of consumer information and tracking sales and preferences at the customer level. Combining government statistics and data from market research firms with geographical data can provide a precise picture of consumer demands. It also might represent an invasion of privacy for individuals. With databases available even to small companies, it is easy to acquire basic data on any individual. For instance, phone numbers and addresses are readily available online. Data collected by governmental agencies such as voter registration and property records can be purchased from several online sources. More comprehensive commercial databases are available from specialty marketing companies. Few laws exist that limit the use of personal data.

It is easy to obtain lists from universities, clubs and social organizations, magazine subscriptions, and mail-order firms. Statistical data can be purchased from the U.S. government. Although most U.S. agencies are forbidden to release specific individual observations until 50 years after the collection date, statistical av-

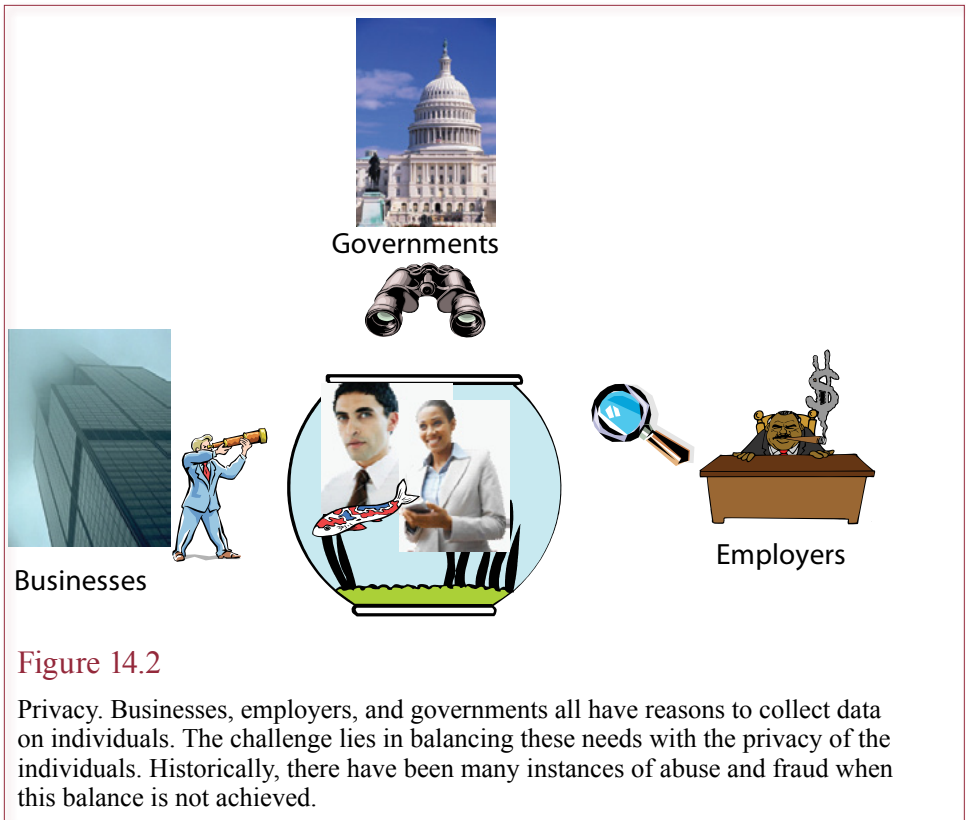


Figure 14.2

Privacy. Businesses, employers, and governments all have reasons to collect data on individuals. The challenge lies in balancing these needs with the privacy of the individuals. Historically, there have been many instances of abuse and fraud when this balance is not achieved.

erages can be highly accurate. By combining the statistical averages with your address, your actual income might be estimated to within a few thousand dollars.

Because most people prefer to maintain their privacy, companies have an ethical (and sometimes legal) obligation to respect their wishes. Individuals can always ask companies not to distribute personal data. Companies should give consumers the option of protecting personal data by building the option into their databases and informing consumers whenever companies collect data.

Consumer Privacy

As shown in Figure 14.3, a tremendous amount of data is collected on consumers. In the early years, consumer activists primarily worried about government data collection. Governments had computers and the authority to force citizens to provide data. Today, businesses can easily collect, obtain, and integrate almost the same level of data available to government agencies. In fact, government agencies have begun using commercial databases in some cases. Credit card and credit bureau data are the two most detailed sources of consumer data.

Consumers have little control over the collection of personal data. But it is interesting how cheaply people will give up their privacy. Grocery store loyalty cards collect a tremendous amount of personal purchase data. Customers routinely sign up for the cards in exchange for a tiny discount on prices. The purchase data is sold to marketing companies and manufacturers to track sales and the success of marketing campaigns.

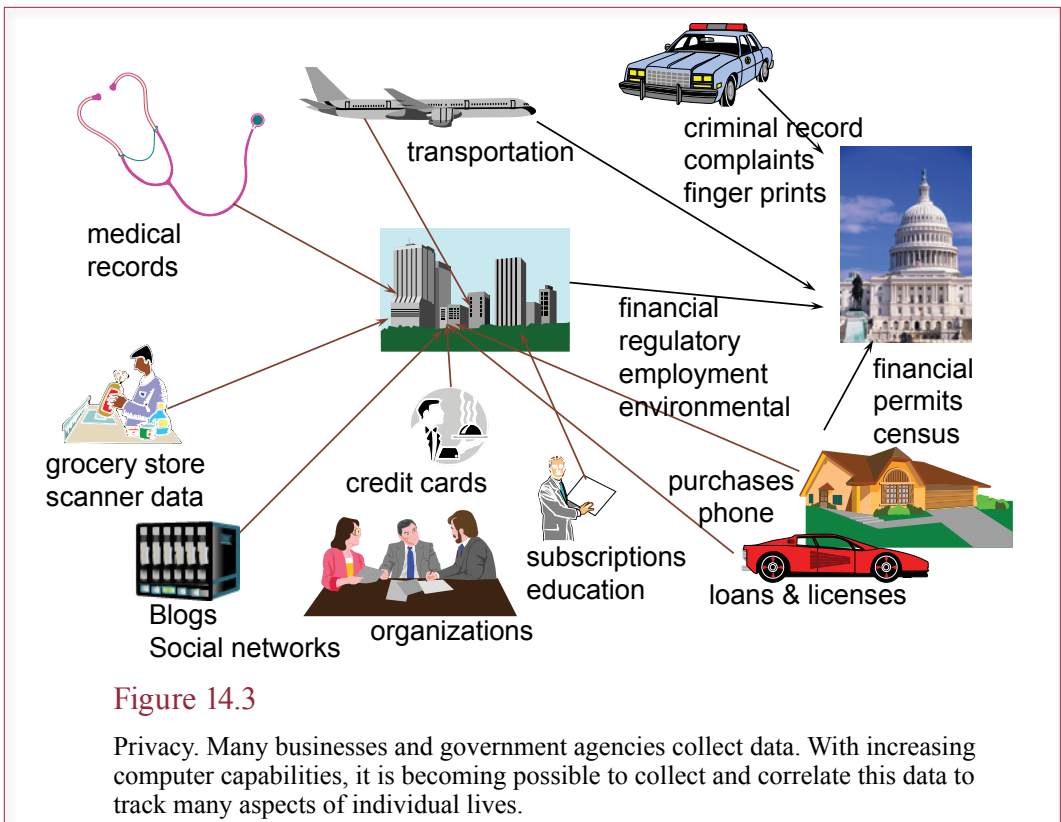


Figure 14.3

Privacy. Many businesses and government agencies collect data. With increasing computer capabilities, it is becoming possible to collect and correlate this data to track many aspects of individual lives.

A significant question remains as to whether consumers really care about their privacy. The loyalty card data and lack of concern over financial records indicate that many people do not care about privacy. Yet over 50 percent of U.S. households signed up for the national do-not-call list to stop telemarketing calls. Perhaps the conclusion is that customers do not mind having data collected, but they do not like being solicited directly.

On the other hand, at times, consumers seem more concerned about online data collection. The technology for Web sites did not initially consider the demands of e-commerce. It was originally intended to simply display pages independently—every request for a page is independent of any other request. For e-commerce, the Web server needs to track information about the person requesting a page. For instance, a shopping cart system needs to store items selected by the customer. Similarly, any site using security needs to track the user through a series of pages—otherwise it would force the user to log in for every new page. These problems were solved with the creation of “magic” **cookies**. A Web cookie is a small text file that the server asks the browser to store on the user’s computer. As shown in Figure 14.4, whenever the browser requests another page from that server, it returns the cookie file containing an identification number. Hence, the server knows which user is returning. This use of cookies is common and relatively benign. Yes, the cookie could be used to track visitors, but presumably the visitor is purchasing items and already willingly provides detailed information to complete the transaction.

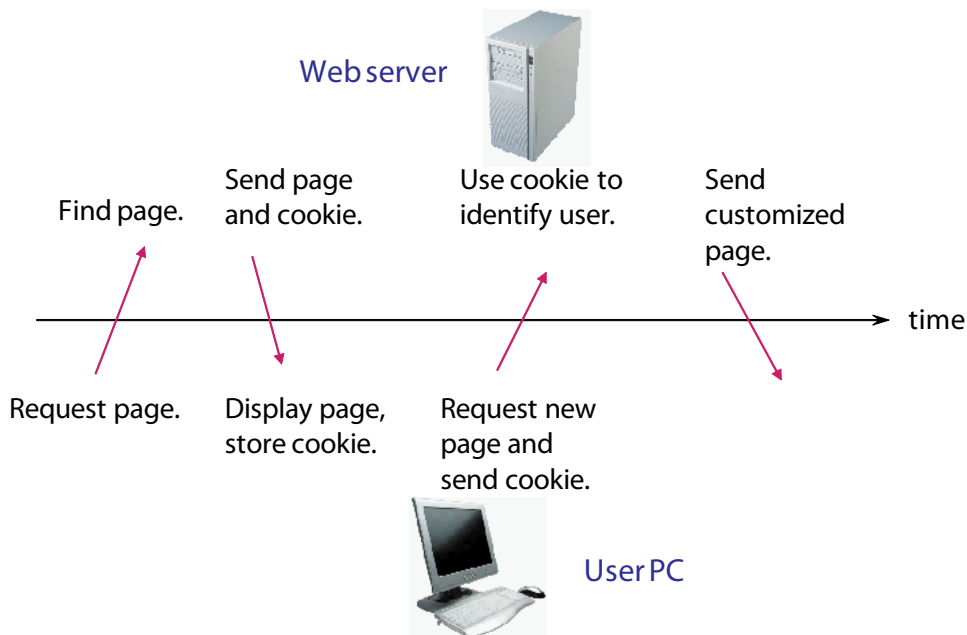
Reality Bytes: Medical Privacy

In early 2011, U.S. Representative Gabrielle Giffords and several others were shot in one of the worst public shooting sprees in the United States. Less than a week later, three employees of the Tucson University Medical Center were fired for accessing the medical records of some of the victims without permission. A nurse working under contract was also fired. The UMC noted that it had installed technology to track unwarranted data access and the three were fired “in accordance with UMC’s zero-tolerance policy on patient privacy violations.” Although most medical workers are careful about patient privacy, this example is not an isolated incident. In April 2009, a Kaiser Permanent hospital near Los Angeles fired 15 workers for accessing medical records of a patient. In 2008, the University of California revealed that over 13 years, as many as 165 medical personnel, including physicians, had improperly accessed records about celebrities.

Adapted from Jaikumar Vijayan, “Three Fired for Accessing Records of Tucson Shooting Victims,” *Computerworld*, January 13, 2011.

Figure 14.4

Web cookies. Cookies are used to keep track of the user across page requests. Each time the user PC requests a page, it returns a small text file (cookie) containing an identification number.



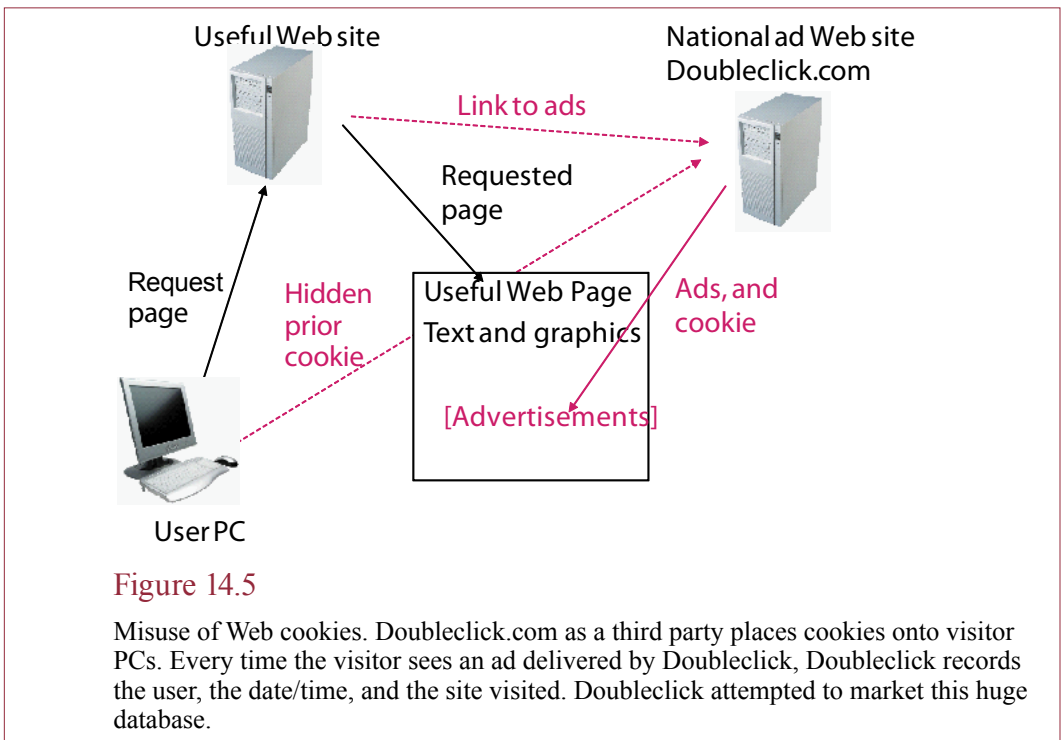


Figure 14.5

Misuse of Web cookies. Doubleclick.com as a third party places cookies onto visitor PCs. Every time the visitor sees an ad delivered by Doubleclick, Doubleclick records the user, the date/time, and the site visited. Doubleclick attempted to market this huge database.

Figure 14.5 shows a more troublesome use of cookies. In 2000, it was revealed that Doubleclick.com (now owned by Google), the leading Web advertisement-placing firm was using cookies as a third party to track page visits by millions of people. Leading Web sites register with Doubleclick to carry advertising. Companies wishing to advertise on the Web create the ad and pay Doubleclick to carry it on its servers. The original Web site includes a link to Doubleclick software that delivers the ads and records page views so that the site owners can be paid the correct fee. However, Doubleclick also includes a cookie that is sent to the visiting PC with each ad placement. Anytime the user visits a site that deals with Doubleclick, the identifying cookie, date/time, and site visited are stored on Doubleclick's servers. Web users were understandably upset when Doubleclick attempted to market this data collection—particularly when the company wanted to tie the online identities to real-world names and addresses. In effect, third-party cookies enable the company to provide information on every site visited by users. In the fall of 2010, the *Wall Street Journal* ran a series of article examining Web sites, cookies, and other tracking devices. Researchers found hundreds of sites tracking users—many of them placing multiple tracking items on user computers.

To prevent this loss of privacy, browsers enable you to turn off cookies—but then you will not be able to use many secure sites, such as those run by banks. Today's browsers offer more control over cookies—in particular, you can refuse to accept third-party cookies such as those placed by Doubleclick. Finding the option is not always easy, but it is one important step to protect your privacy. In 2011, Microsoft and other browser vendors began implementing new ideas for specifying privacy levels in the browser. The main problem is that no Web sites or companies are configured to handle the new methods. And the new methods are not standardized, so it will likely take time before usable privacy controls arrive.

Reality Bytes: Google v. Spain

International laws on privacy are often stronger than those in the United States. For example, the Spanish government has an Agency of Data Protection. The existence of the agency alone is important—it handles citizen complaints about the way their personal data is handled on the Internet. And, the agency has taken a relatively strong position with Google and its search system. The agency claims that Google must delete links to any Web sites that contain information that might compromise an individual's right to privacy. For example, whenever citizens find embarrassing information about themselves on the Web, they can petition to have Google remove any links to that data. In a legal case before the Spanish courts, Google argues that the privacy agency does not force news agencies to remove any of the content. Other countries target the original news source rather than the search engines.

Adapted From David Roman, "Google Contests Spain's Privacy Laws," *The Wall Street Journal*, January 17, 2011.

Wireless technologies offer even more methods for tracking people. Did you know that over 50 percent of emergency calls are made on cell phones? The federal e-911 law requires cell phone operators to provide location data on cell phones. Manufacturers have embedded GPS locator chips within cell phones. Triangulation and signal strength are also used as backup methods. While this data is useful for emergencies, it could also be used for commercial purposes. The company and Web site Loopt has a system where you and your friends can sign up, so that you can open a map to see where your friends are located. This site is used by other applications to enable tracking of your friends. Other sites such as foursquare encourage people to "check-in" to stores to indicate their location to friends, and the rest of the world.

In the realm of autos, GM's On-Star system has been around for years and it tracks the location of your car at all times—for a monthly fee. In 2011, insurance companies in some states began offering discounts to customers who install driving monitors in their cars—not only tracking location but also how you drive. As an individual, do you care if you are tracked? Keep in mind that any stored data can be retrieved by the police or by lawyers in a court case. This data has played a role for both prosecution and defense attorneys in some high-profile cases. But, if you are a completely honest person, perhaps the tracking systems could be good—they might be useful for proving your innocence if you are falsely accused of something—by the police or by your girlfriend/boyfriend.

Imagine the commercial opportunities of broadcasting messages to consumer cell phones as they walk by your store. Now, ask yourself whether you want to be continually interrupted as you walk through the mall, and whether you want stores to be able to track that you walked by the store. On the other hand, the same technology could be used to broadcast emergency messages to any cell phone within a danger zone (fire, tsunami, terrorist attack, and so on).

Employee Privacy

Computers have created other problems with respect to individual privacy. They are sometimes used to monitor employees. Computers can automatically track all of the work done by each person. Some employers post this data on public bul-

Reality Bytes: Hard to Claim Benevolence When You Take Away The Internet

In the “Arab Spring” of 2011, unrest in North African nations led to political changes in many countries. Tunisia was one of the first nations to remove its longtime leader. Egyptian citizens quickly began to follow—with protests and talk of overthrowing long-time leader Mubarek. Mubarek, and many other leaders, believed that the Internet and cell phones were providing communication tools to dissidents. So, by January 28, 2011, the Egyptian government shut down virtually all networks in Egypt. James Cowie, CTO at Internet monitoring firm Renesys noted that “This is on a different level entirely. There’s no cutting off the finger to save the patient here. This really is the Armageddon approach.” In a developed nation like Egypt, the Internet is not just a tool for the wealthy—it has become part of the way business is conducted. And, Internet connections are relatively robust. About the only way to shut down everything was for an official to call all of the ISPs and demand they cease operations. But, shutting down the entire local Internet affects the entire country. That message alone would likely encourage the rest of the population to question the control and intentions of the leaders. A few days later, Mubarek resigned. Internet access and cell phone networks were eventually restored. Iran is another nation that is going even further to control the Internet. The leaders are building a new “national Internet” that would be completely under the control of the government. Reza Begheri Asl, director of the Iranian telecommunication ministry’s research institute said that almost 60 percent of the homes and businesses are on the new network and within two years it would cover the entire country. Some reports say the regime plans to roll out a new operating system to replace Microsoft Windows. Abdolmajid Riazi, when he was deputy director of communication technology in the ministry of telecommunications, said that “It will instead empower Iran and protect its society from cultural invasion and threats. Top officials have said that they consider Western culture and ideas to be a major threat. Cuba currently runs a dual-Internet system, one for the government (and tourists) and a local public one with limited access. The U.S. State Department funds the development of tools to help bypass Internet censorship.

Adapted from Jaikumar Vijayan, “Egypt’s ‘Net Blockage an ‘Armageddon Approach,’” *Computerworld*, January 28, 2011; and Christopher Rhoads and Farnaz Fassihi, “Iran Vows to Unplug Internet,” *The Wall Street Journal*, May 28, 2011.

letin boards to encourage employees to work harder. Some software available for local area networks enables managers to see exactly what every employee is doing—without the employees knowing they are being watched. Some employers read their employees’ electronic-mail messages. Currently, all of these activities are legal in the United States.

Many companies use electronic badges, which employees use to unlock doors. The systems are run by a centralized computer that can be programmed to allow access to specific people only during certain hours. These systems enable employers to track the daily movements of all employees—including the amount of time spent in the restroom.

Courts have repeatedly held that property owned by the employer is completely within its control. Hence, employers have the right to impose any controls or monitoring they wish; as long as they do not violate other laws, such as the discrimination laws.

Reality Bytes: Should Public Data be Private?

Many people are unaware of the amount of public data collected—or aware that it is public. Basic items such as birth, death, and marriage records are recorded publicly—typically at county offices. This data was originally considered to be public so that people could verify the identity of others. In essence, you register with the local government, and it vouches for your identity. Property and some debt records are recorded publicly so that ownership can be verified. Criminal data is public so citizens can recognize lawbreakers. Originally, the files were on paper, and local newspapers would report on the items of interest to the local citizens. Then companies started retrieving the data and putting it online. Leading to cases where a person with a speeding ticket can Google his or her name and see not only the ticket and fine but personal information such as driver's license number and date of birth. The rules about what can be done with public data vary by state.

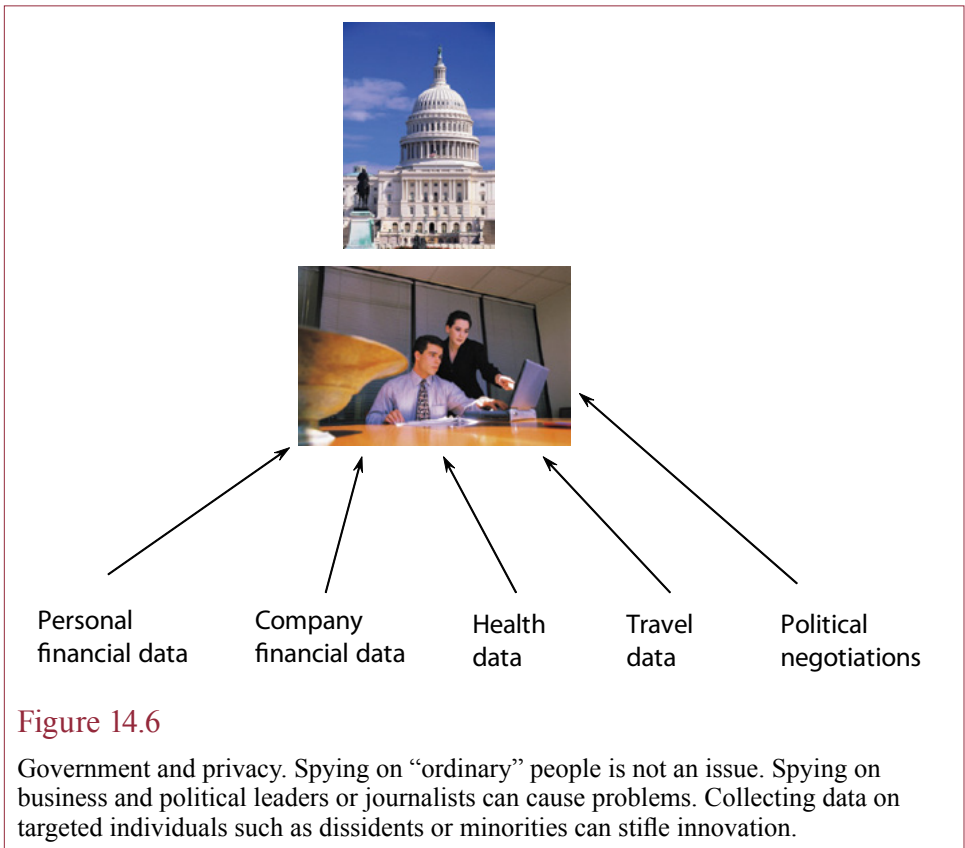
Adapted from Elizabeth Garone, "Help, Google Knows About My Speeding Ticket," *The Wall Street Journal*, February 3, 2011.

It is easy to question why employers might feel the need to monitor their employees. At some point, you have to trust your employees to do their jobs. If an employee has so little work to do that he or she can "waste time using the Internet for personal use," the bigger problem is money the company is wasting on an unneeded employee. On the other hand, most major financial losses come from insiders such as employees and consultants. Furthermore, many companies have been burned by criminals when the companies were not careful enough in hiring and monitoring. Other industries have specific requirements that almost mandate they monitor employees. For instance, the brokerage industry has many regulations dealing with customer contacts, so it routinely monitors employee e-mail messages and phone calls to ensure rules are followed.

Government Privacy

Privacy from government agencies and their employees can be a touchy issue. As citizens, we agree to cooperate with government agencies to improve all of our lives. And to function properly, government agencies can require detailed personal data. For example, as shown in Figure 14.6, most governments collect health data, police records, driving records, international travel, and detailed financial data for taxes. Recipients of federal programs, such as farm subsidies, must report business data. Many people are also required to complete census surveys collecting detailed information about their lives. In the United States, much of this data is protected and can be shared or released only under specific conditions. But there have been several cases of government employees illegally browsing through records for their neighbors or even selling data. In 1991, 18 people were accused of selling Social Security information, including six government employees (*Government Computer News*, January 6, 1992, p. 58).

In the United States, few laws or regulations control the use of data held by private organizations. However, several federal laws control the use of data collected by government agencies. For example, federal agencies are restricted from sharing databases except in specific situations. In most cases the FBI cannot access the IRS data without special permits. In terms of collection and use of data by private



companies, few restrictions exist. Contrary to popular belief, there is no “right to privacy” specified in federal law. However, an element of privacy is contained in a few scattered federal laws and some state laws, and in some Supreme Court interpretations. For example, one federal law prohibits movie rental stores (and libraries) from disclosing lists of items rented by individuals. But this law was largely voided by the Patriot Act of 2001.

As everyone was reminded on September 11, 2001, the flip side to privacy is the need for governments to identify and track individuals to prevent crimes and terrorism. As an open society, the United States has chosen to lean toward individual rights and privacy; but many people have suggested that more control and less privacy would make it easier to stop potential terrorists and criminals. Because of the capabilities of modern information systems and networks, it is now possible to build powerful systems that identify and track individuals within the nation and around the world. Some people have suggested that the United States should establish national identity cards, as used in many European nations. A single, unified database would make it easier to track individual actions.

People tend to be split on the issues of government privacy. Some hate the fact that they have to provide data. Others wonder what the problem is: if you tell your friends how much money you make, why not tell the government? In one sense, public information keeps everyone honest. And for many people, it probably does not matter if various government agencies collect personal data. No one really cares about the personal details of the housewife in Peoria. On the other hand,

Reality Bytes: Google Tracks Police Requests

As a leading portal to the Internet, Google is used by everyone. And, in a twist on the old adage “You are what you eat,” the digital version has become: “You are what you Google.” If someone looked at all of your searches, they could identify what you are working on, planning, or perhaps even thinking. So, the police are increasingly getting Court warrants to obtain Google search data. Agents from other countries place additional requests on Google. In 2010, Google set up an online site to display the frequency of these requests so citizens could see the increasing importance. In the first half of 2010 alone, Google counted more than 4,200 requests in the United States (the country with the largest number of requests). As mobile computing becomes mainstream, police also turn to the cell-phone providers, not just to obtain calling data, but also e-mail and text messages. In 2007, Verizon reported to Congress that it receives 90,000 requests a year. In 2009, Facebook told Newsweek that it received 10 to 20 subpoenas and court orders a day. The U.S. Justice Department has argued in a Colorado Court that it should be able to access e-mails without a search warrant. Does it matter? Ryan Calo, director of the consumer privacy project at the Center for Internet & Society at Stanford Law School notes that “When your job is to protect us by fighting and prosecuting crime, you want every tool available. No one thinks D.O.J. and other investigative agencies are sitting there twisting their mustache trying to violate civil liberties. They’re trying to do their job.”

Adapted from Miguel Helft and Claire Cain Miller, “1986 Privacy Law is Outrun by the Web,” *The New York Times*, January 9, 2011.

some people within governments have abused their positions in the past. Consider the tales of J. Edgar Hoover, longtime head of the FBI. He was obsessed with collecting data on people and built files on tens of thousands of people. Ostensibly he was attempting to remove “subversives” and was a leading cause of the McCarthy anticommunism hearings in the 1950s. He also collected thousands of secret files on politicians, journalists, and business leaders. He used these files to harass and blackmail leaders. Even if a modern-day data collector is not as blatant as Hoover, and even if modern politicians have fewer moral problems, there is still an important risk. What if a politician tries to spy on or interfere with political negotiations? CIA records released in 2007 also reveal the extent of then-president Johnson’s use of the CIA to illegally spy on U.S. citizens in the 1960s and 1970s. He used the “communist threat” to justify spying on college students, journalists, and others participating in the anti-war movement. The same “terrorist threat” could be invoked whenever some politician or police agent decides he or she wants to spy on people. Only now, the spying could easily obtain almost any information about your life—by tracking your cell phone location, your purchases, your car, the material you download and messages you send, your location at work (through employee badge data), in addition to tracking you directly with advanced tracking devices, satellites, and sensors. But, terrorists still walk free.

Some local governments, particularly in the U.S. and England, have become so frustrated with crime that they have installed video cameras on every corner and in every police car. By digitizing the video feeds, automated tools can watch and listen to many events simultaneously. Any potential crimes can be flagged and brought to the attention of a human guard. Beyond the deterrence effect, the data

Reality Bytes: Opt Out Lists

Stop telemarketing phone calls:
www.donotcall.gov

Stop some junk mail:
Mail Preference Service
Direct Marketing Association
PO Box 643
Carmel, NY 10512

Stop credit agencies from selling your address to credit card companies:
Credit Bureau Screen Service
888-567-8688

records are also useful for identifying and prosecuting criminals. But, what will happen when face recognition technology improves and an automated system can track every person every day? Try reading some science fiction novels, such as *Colossus*, for a few ideas.

Protecting Your Privacy

Despite the shortage of laws, you can take several actions to protect your privacy and restrict access to personal data. First, it is your responsibility to direct employers and companies you deal with to not distribute your personal data. You can also ask them why they need personal data and whether it is optional or required. In particular, all federal agencies are required to explain why they need data from you and the purposes for which it will be used. You can also write to direct-marketing associations and file a request that your name not be included in general mailings or unsolicited phone calls. By using variations of your name or address, such as changing your middle initial, you can keep track of which organizations are selling personal data. In some cases, you can refuse to give out personal data (such as a Social Security or taxpayer identification number). If a private company insists, simply stop doing business with it. In a world where firms increasingly rely on a single number for identification, it is important that you protect that number.

With most government agencies and with banks, creditors, and credit-reporting agencies, you have the ability to check any data that refers to you. You have the right to disagree with any inaccurate data and request that it be changed. You can also file letters of explanation that are reported with the original data. In 1994, Congress updated the Fair Credit Reporting Act of 1970. The new version requires credit bureaus to verify disputed information within 30 days or delete it. Businesses that provide data to the credit agencies would also be required to investigate claims of incorrect information. The bill also limits who can have access to the data stored by the credit agencies and controls how it can be used in direct marketing campaigns. In 1994, according to the Associated Press, the bureaus processed 450 million files, selling 1.5 million records a day and handling almost 2 billion pieces of data every month.

Reality Bytes: Pineda v. Williams-Sonoma and Her ZIP Code

A common thread in marketing is to identify your customers. One simple approach is to ask them for a ZIP Code when customers check out. Most people assume the data is needed by the credit card company, but it is not. It is just used to track customers. Detailed Census data can then be paired with the ZIP codes to estimate income and other statistics about customers. Yet, some customers feel pressured when asked for personal data. In California, it is no longer legal for retailers to ask for personal data. A 1990 state law prohibits merchants from recording personal identification information; but merchants commonly ignored it—at least in terms of the ZIP code. In 2009, Jessica Pineda purchased items at a Williams-Sonoma store which asked for her ZIP code. The merchant then used her credit-card number and ZIP Code to retrieve her home address and add her to the catalog list. She began receiving catalogs and other mail from the company. It is likely that the vendor also sold her information to other companies. In 2011, the California Supreme Court ruled that a ZIP Code constitutes “personal information” and it is illegal for merchants to ask for it. A ZIP Code might seem innocent, but with huge databases, it seems that ZIP Code, gender, and birthdate are sufficient to identify most people.

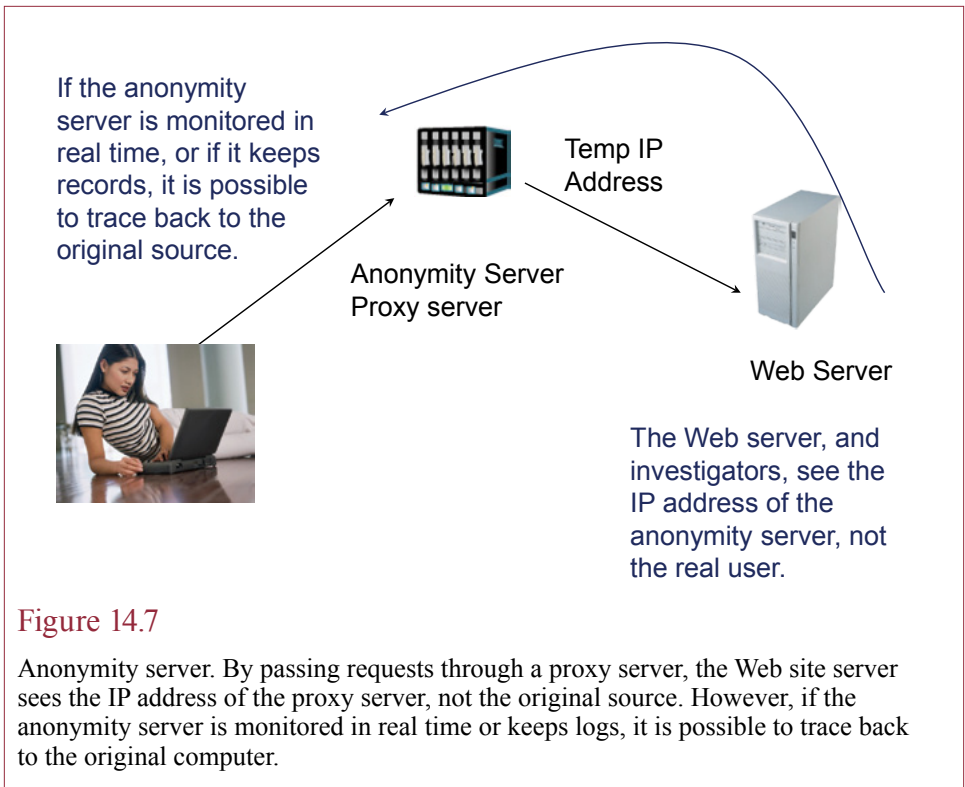
Adapted from Scott Thurm, “California Court Says Stores Can’t Ask for ZIP Codes,” *The Wall Street Journal*, February 10, 2011.

Privacy Laws and Rules

The United States has few laws regarding privacy, although a few states do offer some stronger protections. On the federal level, the Bork Bill states that video rental stores and libraries cannot release their rental data. It was passed by Congress when some over-zealous reporters obtained the video rental records of a judge nominee (Bork). The 1974 Family Educational Privacy Act prohibits schools from releasing grade data without permission from the student. The Privacy Act of 1994 placed some minimal limits on the sales of state and local driver’s license data. The Privacy Act of 1974 limits what data can be collected and shared by federal agencies. However, various rules, interpretations, and practices have created enough loopholes to circumvent most of the original provisions.

In terms of financial data, various laws give consumers the ability to obtain their credit records once a year and the right to dispute items in the report and have the dispute resolved within 30 days. In 2001, a federal rule took effect that was initiated by President Clinton to provide some control over the use of medical data. Health care providers already complained about the high cost of implementing the provisions, and some of the provisions were withdrawn when George W. Bush became president. Nominally, the rules state that transfer of data (particularly prescription drug data) requires permission from the patient. However, most healthcare organizations require customers to sign waivers enabling them to share data.

In contrast to the United States, the European Union has stronger consumer privacy laws. Most EU nations have adopted the European commission’s 1995 Data Protection Directive. Since 1978, France has had its own strict Data Protection Act. The laws basically state that personal data can be collected only with the user’s permission, the user must be clearly told how the data will be used, and the



user has the right to see and to change any personal data. The laws have an additional important condition: personal consumer data cannot be moved to a nation with lesser privacy controls—notably the United States. The United States has negotiated a loose “safe harbor” provision, so that companies can bring European consumer data to the United States if the companies formally agree to abide by the EU directives and also agree not to resell the data. These provisions make it more expensive to collect data in Europe—sometimes beyond the price of small businesses. For example, in the United States, it is relatively easy to purchase e-mail lists of potential customers for a few hundred dollars. In Europe, these lists would generally be illegal to use, since the customer did not agree to the unsolicited use of his or her address.

Anonymity

Anonymity is the flip side of the privacy question. Until recently, it has been difficult or impossible to provide anonymous access to the Internet. Using advanced encryption, some firms now offer people the ability to use the Internet without revealing any data about themselves. Remember that the Internet works by assigning IP addresses to all computers. Any server that you visit saves your IP address in log files. It can be somewhat difficult to match an IP address to a specific individual, but it provides a general location. If necessary, a court order can be obtained to track an IP address to a specific individual. However, Figure 14.7 shows that a proxy server can hide your IP address. Sites that you visit see only the address of the intermediate server. The server also intercepts all cookies and

other files sent by some servers. However, if the anonymity server keeps logs or if it is monitored in real time as data is being transferred, it is easy to trace sessions back to the original source. The primary U.S. wire-tapping law, Communication Assistance for Law Enforcement Act of 1994 (CALEA), was interpreted in 2006 to require that all ISPs must provide the ability to invisibly tap Internet connections and provide real-time feeds to a law enforcement agency when ordered by a court. Because of these laws, truly anonymous servers cannot exist within the United States, but a few are run by various people around the world. It is not clear whether they can be monitored in real time or are subject to court-ordered retrieval of data.

The ultimate question that you, as an important member of society, must answer is whether anonymity should be allowed, or how it should be controlled. Certainly it can be used to improve privacy. People who have a stronger belief in personal privacy might seek out and use anonymity servers—others will decide that privacy is not an issue. But what about drug dealers, terrorists, child pornographers, and other illegal activities that society wishes to stop? Or what about anonymous harassment? Someone could use the technology to harass and intimidate people on the Internet. Perhaps society should not allow anonymity? On the flip side, who makes that decision? If some nation chooses to ban dissenting viewpoints, or if a government whistleblower needs to protect a career or a life, anonymous sites can be valuable tools to increase information and open discussions.

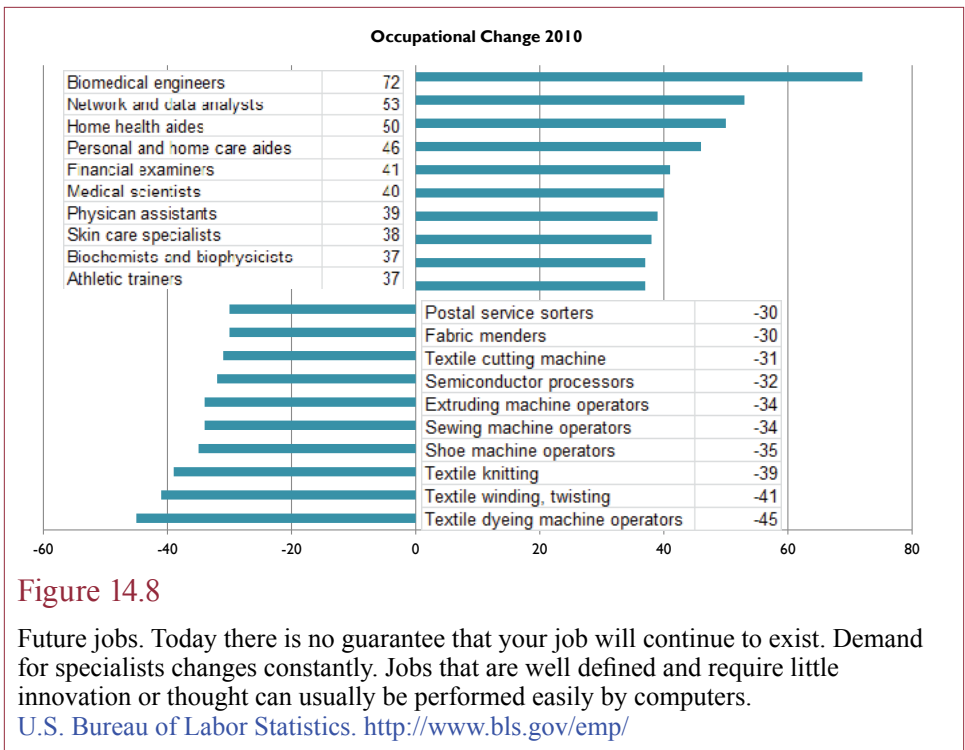
Jobs

How does technology affect jobs? If computers do more of the work, what jobs are left for people? Technology can affect jobs in other ways as well. It opens up the world to people with physical disabilities. By removing location as an issue, networks make it possible to work on jobs from almost anywhere in the world. You can telecommute or consult around the world without leaving your home.

Loss of Jobs

There is no question that technology causes some workers to lose their jobs. In the 19th century, Luddites reacted to textile automation by destroying machines. Information technology is no exception. Norbert Weiner, a computer pioneer in the 1940s, predicted a major depression would result from computers replacing workers. Despite these predictions, during the last 100 years technology has increased the number of jobs and raised the standard of living for most workers. Since the introduction of computers in the 1950s, the world's economies have grown and incomes have increased. However, individual workers can lose jobs in the short run. Even in the long run, lower-skilled workers experience greater difficulty in finding new jobs. Compare the automated shipyards of Singapore to those in the United States. In Singapore, one man using computer screens and a joystick moves hundreds of containerized cargoes without ever leaving his office. In the United States, each crane requires a crew of four workers, including one just to identify shipments and destinations that are handled by computer in Singapore. In Europe, the Dutch port in Rotterdam cut employment in half by installing robotic cranes and automated transfer vehicles.

The point is that some jobs will disappear, but others will take their place. In the shipyard example, more technical expertise will be needed to program and repair the equipment. Figure 14.8 shows the changes in jobs for the next few years



that are anticipated by the Bureau of Labor Statistics. Although they do not make the top-ten list in 2010, a few of the fastest growing jobs are in computer technology. But due to outsourcing and cost issues, the list is shorter now than it was a couple of years ago.

Most economic experts believe that technology increases the total number of jobs. New technology creates demand for people to design it, manufacturing firms to produce it, and people to maintain and repair it. Computer hardware also creates demand for software programmers. More important, technology can cause the economy to grow, creating more jobs in all sectors. By most indications, new jobs created by technology tend to be higher paying, physically safer, and less repetitive than those replaced by technology. Information technology can also reduce product prices, raising the standard of living by enabling people to buy more goods. On the other hand, technology typically causes some workers to lose their jobs. Unfortunately, many of these displaced workers cannot be retrained for the new jobs created by the technology. Similarly, the new jobs might pay less money, have lower status, or might have less desirable work environments. As computers and software become increasingly powerful and intelligent, it encroaches on even more jobs. The U.S. recession starting in 2008 resulted in many companies reducing the number of workers—particularly in middle management.

Governments have created several programs to provide benefits of money, retraining, and relocation to workers who lose their jobs. Managers need to understand the effects on employees when new technology is introduced. Many corporations provide ongoing educational payments and training classes to help workers improve their skills. Others provide out placement services to help unemployed workers in their job search.

As individuals, we need to remember that changing technology can eliminate virtually any job. One of the best plans is to continue your education and learn new skills. Remember that technology continually changes. Some of the skills you learn today will be obsolete in a couple of years. We must all continually learn new skills and adapt to changes. Applying these skills in your current job adds experience that will help you find a new job. It also benefits your current employer and might help you keep your job or stay with the company if new technology makes your current job obsolete.

The concept of continually acquiring new skills sounds straightforward. However, many times you will have to choose among multiple technologies. Guessing wrong can lead you to invest time and money in a technology or skill that fades away. As you become more involved with technology, you will increasingly find it necessary to “predict” the future. Identifying trends and deciphering fact from rumor are important skills to learn.

Physical Disabilities

Technology offers many possibilities to provide jobs for workers with physical disabilities. In fact, in 1992, the U.S. Congress passed the Americans with Disabilities Act, stating that companies are not allowed to discriminate against disabled employees. Common uses of technology include the use of scanners and speech synthesizers for visually impaired workers; voice input devices and graphics displays for workers who cannot use keyboards; and telecommuting for those who work from home. In 2001, the U.S. government began requiring that all software it purchases must be accessible to users with disabilities. Since the federal government employs hundreds of thousands of workers, this order should encourage all software providers to improve their software.

Most Windows-based software contains features to facilitate usage by people with various physical challenges. In some cases, additional accessibility tools can be downloaded or purchased to provide more features. Speech recognition packages are useful for many applications. Sometimes adaptive devices are needed to provide alternative ways to enter data and obtain the results.

Web sites still present accessibility problems, particularly for those with visual impairments. Many sites rely on color and graphics, which are difficult for the accessibility tools to interpret. These issues are being discussed by many vendors. Check Microsoft’s accessibility site for more details.

Telecommuting

The fact that about 70 percent of U.S. jobs are service-based raises interesting possibilities for workers. Many services like accounting, legal advice, education, insurance, investments, data analysis, computer programming, and consulting are not tied to a physical location. As a service provider, you could be located anywhere and still perform your job—as long as you have the appropriate telecommunications system. As communication improves to include video links and faster document transfer, even more jobs can be performed from remote locations.

Some companies are experimenting with home-based workers, especially in cities such as Los Angeles and New York with long commute times. Some workers like the concept; others try it for a few months and return to a traditional workplace job. Several advantages and complications arise from the perspective of the worker, the firm, and society.

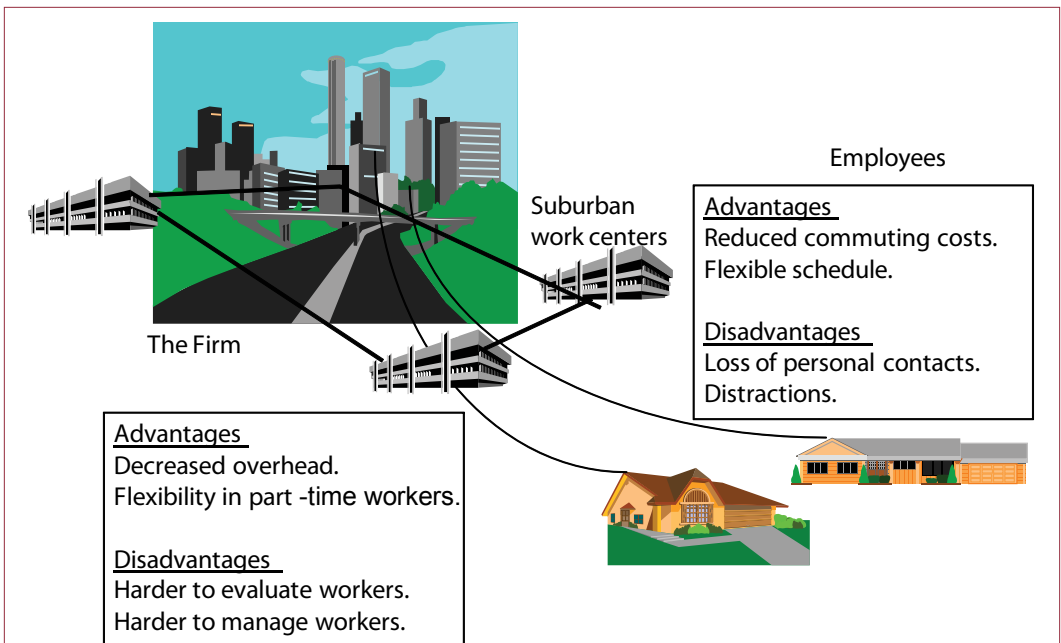


Figure 14.9

Telecommuting. In the simplest form of telecommuting, individual workers connect to office computers from their homes. An intermediate method has been used to avoid the problems of distractions and the cost of creating a home office. Workers report to satellite centers in their suburban neighborhood. Workers retain a structured environment but reduce their travel time.

If a substantial number of workers choose to work from home, the firm gains two main advantages: (1) decreased costs through smaller offices, and (2) flexibility in hiring additional workers on a contract basis. Some people have predicted that companies might also gain from increased use of part-time workers, thus avoiding the cost of insurance and other benefits. The greatest complication to the firm is evaluating and managing employees. Without daily personal contact, including conversations, it is harder to spot problems and make informal suggestions as corrections.

To the worker, the most obvious benefit lies in reducing the time and expense of commuting to work. The biggest drawback lies in the loss of personal contact and daily ritual of a typical work schedule. Depending on your home environment, there can be substantially more interruptions and distractions at home. It is also more difficult to “get away” from your job. Working from home on a flexible schedule requires strong motivation and organization. Before you choose to work at home, talk to someone with experience.

A few firms have experimented with intermediate telecommuting options. As indicated in Figure 14.9, the firm leases smaller offices in city suburbs and workers operate from these satellite offices instead of one central location. The offices are linked by high-capacity telecommunication lines. Workers keep a traditional office environment but cut their commuting costs. Businesses maintain traditional management control but do not save as much money.

A few people have speculated about the effects on society if there is a large shift to telecommuting. At this point, there is not much evidence to support any of the hypotheses, but many of them focus on negative aspects. People could become isolated. Jobs could become highly competitive and short-term. Firms could list projects on the network and workers would compete for every job. Workers would essentially become independent contractors and bear the responsibilities and costs of insurance, retirement, and other benefits, with little or no job security. They would also have no loyalty to any particular firm. Firms could become loose coalitions of workers and teams that are constantly changing, with little control over future directions. It is hard to predict what will really happen, but by understanding the negative effects, they become easier to avoid.

Business: Vendors and Consumers

How does technology change the relationship between businesses and consumers? Business consists of transactions. Changes in the way transactions are handled can alter society. In particular, as digital content becomes more important, can the existing laws created decades ago still be applied? And if the laws are replaced, will they affect the balance of power in the relationship between vendors and consumers?

Intellectual Property

Intellectual property is the general term to describe ownership of ideas (patents) and creative expressions (copyrights). For many years, there was a solid distinction between the two: ideas involving physical items (such as machines) could be patented. A **patent** essentially grants a monopoly to an inventor for a fixed period of time (originally 17 years in the United States but now 20 years). During that time, no other company can introduce a similar device—even if the second creator did not use any knowledge from the first inventor. A **copyright** is created for other creative works—traditionally writing and music. It protects the specific article from being copied and grants the owner the sole right to create derivative works (such as a sequel). But it does not prevent others from creating similar works. For example, one person could write a story about space explorers. Someone else could also write a story about space explorers, and it would not be an infringement on the first story. If the second story used the same characters and plot, it might be an infringement, but it might not, depending on the interpretation of the courts. In the mid-1990s, the U.S. patent office began granting patents for nonphysical items—specifically for business ideas. Patents were supposed to be granted only for nontrivial ideas, but for a while, the patent office got carried away and forgot that patents are only supposed to be granted for “nontrivial and nonobvious” inventions. For instance, it granted a business process patent to Amazon.com for one-click checkout of Web sales; so no other Web site was allowed to offer a checkout system with a single click without paying royalties to Amazon.

The goal of patents and copyrights is to encourage creativity by offering protected rewards to innovators. Remember from economics that without a barrier to entry, any firm that makes a profit will attract competitors. Patents and copyrights are designed to be barriers to entry for a limited time. But the laws were written in decades when the goal was to protect companies from other companies. For instance, before computers, only a large company would be able to copy a book and reprint it. The laws made it clear that this action was illegal, and the injured party could easily find and sue the single violator for damages. Several exemptions to

Reality Bytes: Cignet and Massachusetts General Fined for HIPAA Violations

The U.S. Department of Health and Human Services (HHS) is in charge of enforcing the provisions of the Health Insurance Portability and Accountability Act (HIPAA). Two major features of the rules are that patients can receive copies of their health records and that medical institutions must protect the privacy of patient data. In 2011, HHS completed enforcement actions against two companies based on separate violations of those provisions. The insurance company Cignet had failed to provide records to patients in a timely manner. The company also failed to cooperate with investigations and to produce records to HHS. Cignet paid a \$1.3 million penalty. Massachusetts General Hospital faced a different problem. In March 2009, an employee of the Hospital accidentally left health documents for 192 patients on a subway train. The Hospital ended up paying HHS \$1 million in fines. The two actions represent the first fines imposed due to HIPAA. Perhaps the actions will help convince businesses to protect customer data. But much remains to be done. A report from the accounting firm Kaufman, Rossin & Co. revealed that in 2010 businesses somehow gave up or lost health data on about 5 million patients.

Adapted From Jaikumar Vijayan, "HIPAA Privacy Actions Seen as Warning," *The Wall Street Journal*, February 25, 2011.

the copyright law were specifically created to support important noninfringing uses that are considered valuable to society. For example, educational institutions can make limited copies of items for discussion and research.

The basic laws made sense when large companies were the primary threats to copying products and content. Only large print shops, music firms, and competitors had the money, tools, and distribution networks to become a serious threat. For example, the music industry did not consider cassette tape copies made by individuals as a serious threat.

Digital content changed most of the underlying assumptions of the intellectual property discussion. First, it is easy for anyone to make perfect copies. Second, it is equally easy for everyone to distribute those copies—at virtually no cost. Instead of a large competitor, now the threat is millions of your own customers. Some of these issues are cultural and economic. For example, some industry-sponsored reports indicate that software piracy in Southeast Asia is huge: over 90 percent of software in use is copied. Nations such as Vietnam do not have the tradition of paying for creative works, and do not have much money to pay for them.

The most famous case of these copyright issues involved the company called Napster. Napster was a pure Internet firm that ran a Web site to make it easy for consumers to find and share digital music files. In an attempt to stay within the copyright laws, Napster did not store any files and did not charge for its services. Instead, it was simply a giant directory. Individuals searching for specific songs went to the Napster site, found a fellow enthusiast with a desired file, and copied the file from the other's machine. Napster lost the ensuing lawsuit from the music industry. But the battle is far from over. Napster made it easy by providing a single target to sue. What if there is no central company directing the copying? One such firm, LimeWire, was shut down in 2011 for violating copyright laws by providing software for "sharing" music.

Technology Toolbox: Privacy

Problem: How do you improve privacy on the Internet?

Tools: Most current browsers have tools for improving privacy by reducing the data exchanged with Web sites. But, browser vendors tend to hide these tools because most receive large amounts of advertising money that might be disrupted. Also, stronger privacy sometimes makes Web sites unusable or harder to use.

Microsoft Internet Explorer (IE) has a couple of privacy controls. The simplest one is to control the use of cookies. In particular, you should disable third-party cookies. These are installed and used almost exclusively by advertising companies such as Double-Click (Google) to track which sites you visit. To disable them, use the main menu (press the Alt key) Tools/Internet Options/Privacy tab, then select the Advanced button. First-party cookies should be set to Accept, and third-party cookies set to Block. If you have problems with some sites, you might set it to Prompt, but that will generate warning messages on almost any site you browse. IE9 and above has a new option under the Privacy tab to “Never allow websites to request your physical location,” that you might want to select. If you are going to browse a Web site for research or where you want to ensure absolutely minimal tracking and minimal history, IE provides the InPrivate browsing mode. Start IE then click the small new tab icon on the tabs row. Find and click the link for “InPrivate Browsing” which will open a new browser window. In this mode, minimal information is exchanged or stored on your computer.

The Google Chrome browser has similar settings under different names. To block third-party cookies, click the Settings icon and choose the Under the Hood tab. In the Privacy section, click the Content Settings button. In the Cookies section, check the option to Ignore exceptions and block third-party cookies. Chrome also has a mode that does not save any cookies, temporary files, or history. Click the Settings icon and pick the New Incognito Window option.

Firefox and IE have a new option to “Tell Web sites I do not want to be tracked.” The problem with this option is that it is not yet a standard and none of the Web sites actually support it. Firefox has a “private browsing” option. Press the Alt key to activate the menu, choose Tools/Start Private browsing.

At the server level, it is also useful to opt out of some Web site tracking. A big one is to opt out of Google: <http://www.google.com/privacy/ads/>, which includes getting rid of Double-Click tracking.

Quick Quiz:

1. Can you prevent Web sites from collecting your personal data?
2. What do you gain by blocking third-party cookies?
3. Why would you not want to use “Private” or “Incognito” browsing all the time?

Reality Bytes: Dirty Politics Goes Online

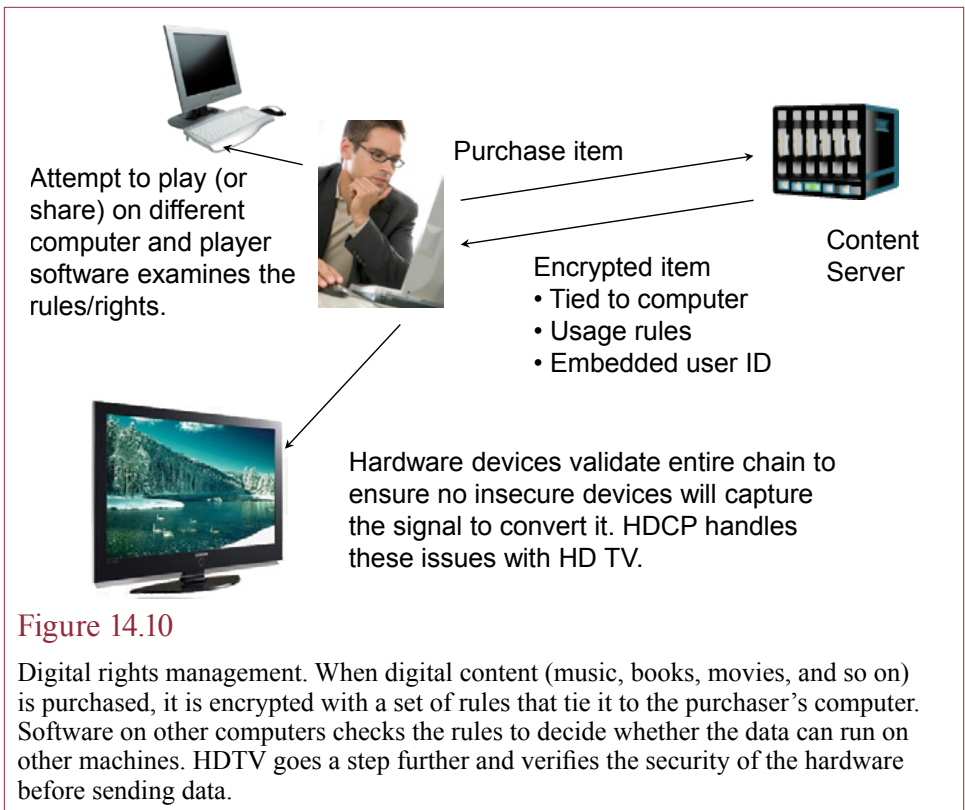
It is unlikely that anyone likes political campaigns, but they are a necessary component of a democratic society. On the other hand, political campaigns that become “dirty” are even more annoying. Apparently, political consultants are now working with technology practitioners to generate online attacks. Someone hacked and released thousands of e-mails from HBGary Federal, a security consulting firm. The messages show that the company pitched ideas to lawyers at Hunton & Williams, a D.C. law and lobbying firm. The ideas included create fake social network accounts to mislead people, scanning Facebook and other accounts to find negative information about opponents, and planting false documents to undermine the credibility of activists. Workers from HBGary Federal, Berico, and Palantir suggested many ways to spread disinformation online. It is not clear whether the actions would be illegal or if any were actually undertaken. But, given the challenges of tracking actions online, it is only a matter of time before dirty tricks become more common.

Adapted from Dan Eggen, “Hacked e-Mails Show Web is an Increasingly Useful Tool in Dirty-Tricks Campaigns,” *The Washington Post*, March 4, 2011.

In response to these problems, content providers began encrypting their content to make it more difficult to share. Cable and satellite TV providers were among the first to scramble their signals to make it more difficult for people to steal the signals. In response, several companies started selling and advertising black boxes that would descramble the signals, making it possible for anyone to steal the TV signals. Technically, it was illegal for people to steal the signal, but it was economically difficult for companies to stop the theft.

To solve this problem and help protect IP rights, the United States passed the Digital Millennium Copyright Act (DMCA). One of the most important changes in the act is a provision that makes it illegal to circumvent any copyright protection scheme. For example, this provision made it illegal for companies to advertise and sell TV descramblers. The law was generally accepted in terms of hardware issues, but problems and complaints quickly arose when circumvention focuses on software and information.

In existing cases, the DMCA provision has been interpreted to mean that any discussion of how to circumvent protection is illegal. The first case pursued under this provision relates to DVD movie disks and the DeCSS program. DVD files are encrypted so that they can be played only on specific machines with authorized software. The files are only weakly protected. Direct from the manufacturer, the files can be copied to other computers, but can only be viewed with the special software. Since that software did not originally exist for some computer systems (notably Linux), a few experts found a way to defeat the encryption. They posted this method (known as DeCSS) on the Internet. The movie studios promptly sued every Web site that carried the program for violating the DMCA. Many people are concerned that these actions violate the spirit of free speech and open discussion. Of course, whether or not the movie industry wins the case is almost irrelevant. One key factor of the Internet is that it is impossible to destroy knowledge once it has been created. Several Web sites in foreign nations that do not support the DMCA carry the information.



Computer software, music and digital books face similar issues. As more content moves online, creators and publishers searched for a stronger solution that will prevent customers from copying and sharing digital data.

Digital Rights Management

Digital rights management (DRM) tools use encryption and rules embedded in the data to control how purchasers can use and transfer data. Figure 14.10 shows the basic concept. Several companies provide DRM tools, leading to different approaches, but many of them follow a similar process that is pushed heavily by Microsoft. When an item is purchased, software on the purchaser's computer creates an identifier for that machine and sends it to the server. The server encrypts the data, embeds a set of rules, and often embeds a user ID. If the content publisher finds an illegal copy of a file online, it can be traced back to the original purchaser. To date, no one has tested this concept in court to see if it could be held against the original purchaser. As a simple defense, the purchaser could argue that a virus or Trojan Horse copied the file invisibly.

For DRM to work the software that plays or displays the file must know how to decrypt the file and it must follow the embedded rules. Even if the file is transferred to a different computer, the software will not play the file if the rules are not met. Most systems accomplish this task by requiring that the file be played with a specific software package. For example, originally files purchased through Apple could be played only with the iTunes software, and files protected with Microsoft DRM could be played only with Microsoft media software. The process becomes

more complicated if the data needs to be compatible with multiple devices created by different manufacturers. HDTV is the primary example. You can buy a Blu-Ray disk created by several companies, play them on several different players and connect the player to any television. To protect the content, all of the manufacturers had to agree on the **high-bandwidth digital content protection (HDCP)** format.

Effective DRM is difficult to create. For example, music eventually is converted to analog form and played through speakers. It is relatively easy to convert it back to digital form that is no longer protected—but some quality might be lost in the process. HDTV took the process a few steps further. The high-definition players examine the entire collection of devices, including the connecting cables, to ensure that all of the devices support HDCP. If not, it plays the video in a lower-quality picture. Some early devices even required the video output to be directly connected to the display device (TV).

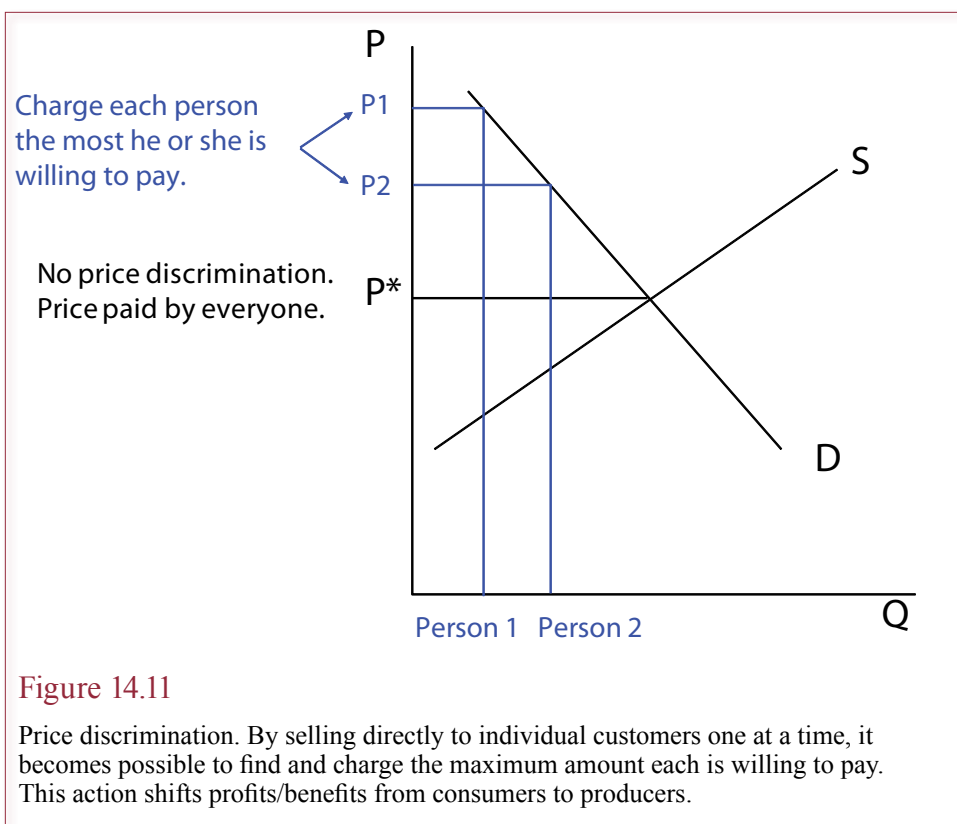
Many people look at DRM as a challenge—something to defeat simply because it is there. In theory, any DRM scheme can be defeated—given enough time and effort. Programmers have full access to the computer so they can trace every step in the process. Technically, DMCA makes these efforts, and publishing it, illegal in the United States; but it will not stop the work.

The flip side of copyrights is the argument that content should be free. But who would take the time to create useful content if it is free to everyone? Stephen King, the noted author, ran an experiment in the late 1990s. He wrote a novella and began writing a novel in installments. He distributed them through his Web site. He attracted hundreds of thousands of visitors and free downloads. He ultimately stopped the projects because of lack of revenue (it was more profitable for him to devote his time to paying projects).

At this time, DRM is a highly contentious issue. It makes life more difficult for honest consumers and limits what they can do with the data they purchased. For example, imagine the problems that can arise if all of your music is locked to one computer and that computer dies. Even if you have backups, you will need special permission to transfer them to a new device. Many companies establish rules to support using the content on three or four computers, but that rule will not cover a lifetime of upgrades. In 2007, Steven Jobs, the CEO of Apple, attempted to convince the music industry to allow him to drop DRM conditions on the songs his company sells.

By 2011, most digital music was sold without copy protection (DRM). Does that mean consumers became more honest? Certainly, it is now easier to purchase music online, particularly individual songs. Some prices have dropped with competition. But, the music industry continues to report declining revenues from all forms of music sales. (For some interesting charts, see <http://www.businessinsider.com/these-charts-explain-the-real-death-of-the-music-industry-2011-2>.)

DRM presents an interesting dilemma to businesses that sell digital content. The fear is that if you do not include DRM, everyone will copy your content and “share” it with others, reducing the number of sales. But, if you do use DRM, you make life more difficult for legitimate users who pay for the product. For example, as of 2011 most book publishers sell DRM-protected books for electronic readers. Effectively, the DRM locks the book to specific devices. Customers run the risk of losing their existing books if they switch to a different device, or even if a device breaks or is lost. In the meantime, the DRM methods were generally broken, with methods available online, within a few months. Additionally, almost anyone could



use a scanner to turn a print copy of a book into an unprotected digital copy in less than an hour. Similar issues face publishers of music, movies, and software. Music moved away from DRM largely because of the decision to avoid locking music to specific devices. Movies continue to cling to DRM. Software varies, with big publishers such as Microsoft and Adobe leading the way with DRM (their software uses Internet connections to limit the number of installations.) Clearly, it is within the rights of the copyright owners (publishers and authors) to choose to implement DRM. Also, in the U.S. the DMCA makes it illegal to circumvent DRM protections (although this provision is largely untested in court). But, from a business perspective, managers need to think about exactly what is gained and lost through DRM.

Balance of Power

Some of the issues with intellectual property arise because of questions of balance of power between the creator, the publisher, the retailer, and the consumers. For instance, the Internet, with its digital content, provides the opportunity for authors and creators to circumvent the traditional publishers. Currently, authors receive only a small portion of the list price of an item. Retailers, distributors, and publishers take the majority of the money. In a world that requires distribution of physical items, these are the costs artists must pay to reach consumers. In a digital world, anyone can sell products directly to consumers. Of course, it will be simpler and more cost-effective when consumers adopt a small-payments mechanism. The point is that the few large publishers in each industry have a strong interest in

Reality Bytes: Poker is Not Gambling?

U.S. law makes it illegal to gamble “by wire” which includes Internet gambling. Online casinos and games of chance were banned shortly after the Web became popular. Federal law prohibits credit card companies from transferring money to online casinos. But, for several years, online poker sites flourished—even in America. Credit card companies did not transfer money to them, but a few banks handled special accounts for them. In April 2011, Federal authorities cracked down on the online poker sites. Initially, eleven people were arrested, including three founders of the largest poker sites. Federal agents filed restraining orders against 76 bank accounts in 14 nations; alleging at least \$3 billion in money-laundering penalties. PokerScout, a site that tracks playing, estimated 1.8 million U.S. players wagered \$16 billion in 2010. About one-third of the money deposited by players ended up going to the online companies as the “rake” or house percentage. Prosecutors also seized five of the Internet domains used by the poker companies, shutting down the services and putting up warning notices. In their defense, the arrested founders argued that the sites are not illegal because poker is not gambling.

Adapted from Alexandra Berzon and Chad Bray, “Eleven Charged in Federal Crackdown on Online-Poker Companies,” *The Wall Street Journal*, April 16, 2011.

maintaining control over the distribution system, so most proposals have catered to these large firms. For example, the DRM systems keep the role of the retailers and the publishers, so the costs to consumers are likely to remain high.

All of these issues are challenging with multiple perspectives. Society needs to protect and encourage innovation because it creates new products and moves the economy and society forward. But, in these cases, technology also makes it easier for individuals to copy and distribute protected works, and it is economically infeasible for an innovator to sue millions of people over patent or copyright violations. The issues also revolve around important economic concepts. Digital content essentially has zero cost to copy and distribute (but high fixed costs to create).

As shown in Figure 14.11, another interesting economic issue is that some people are willing to pay higher prices for the content than others are. In a typical market, the price is determined by supply and demand so that the market clears with no shortages or surpluses. Effectively, everyone pays the same price (or close to it). People who were willing to pay more money for a latest release got a deal (or consumer surplus) because they paid the same fixed price. But, in an online digital world, it is possible that the customer will purchase directly from the producer. Every sale is separate, and individuals might not even know how much others are paying—particularly if you want to buy a newly released item. In this situation, it is possible to set up a system where each customer pays his or her highest price—perhaps through an ongoing series of auctions. For example, if you want to be the first person to download a specific song, you will pay more. If you are willing to wait a few days or weeks, you can pay a lower price. Or, more sophisticated methods could be created. In the end, each person pays a different price, but one that each is willing and able to pay. The balance of power is changed and the producer captures more of the consumer’s money. Is this situation good or bad? The answer depends heavily on your personal beliefs, but it is certainly different. When Amazon tried an experiment several years ago, (the company charged dif-

Can technology improve education?

- Computer-assisted instruction to provide individual attention
- Course management
- Distance learning

Do people want more technology in education?

- Teachers
- Students
- Employers

Are the answers different for lifelong learning?

- Professionals
- Employers
- Military

Figure 14.12

Information technology in education. The technology has the potential to change education, particularly in terms of individualized attention, course management, and distance. But it is expensive and time consuming to provide the infrastructure and create new applications. Nontraditional areas such as continuing professional education (CPE), employer training, and the military have found several benefits in the technologies.

ferent prices for the same book in different cities), customers were unhappy when they found out some people paid a lower price. Apple negotiated with the studios to be able to charge different prices for each song. Popular, newly-released songs cost more than older songs. It is not perfect discrimination, but someday new pricing mechanisms might be introduced that add even more levels of prices.

Education and Training

Can information technology change education? For hundreds of years, the principles and techniques of education have changed only slightly. As new technologies are introduced, people have often declared that the world of education would change markedly. Yet, few technologies have had a lasting impact on education. Television is a classic example. Although movies and news reports are sometimes used for teaching purposes, the role of television in formal education is minimal. However, it is used for informal education and for training, especially with the availability of videotapes for teaching specific tasks. And, as bandwidth has increased, video communication is growing as a way to connect with students in distant locations.

One of the drawbacks to video education is the lack of interaction and feedback. Multimedia tools that combine video, sound, and computer interaction represent one attempt to surmount this limitation. However, three basic problems arise when applying technology to education. First, technology is often expensive, especially compared with traditional methods. Second, it is time consuming to create lessons that generally are difficult to change. Third, there is little conclusive evidence that the techniques are equal to or superior to existing techniques. Especially in light of the first two problems, it is difficult to test the new technologies. In many cases, by the time prices have fallen and lessons are created, an even newer technology emerges.

Despite these obstacles, technological innovations are often used for specialized teaching purposes. For instance, interactive and multimedia computer tools can be used to provide more in-depth study for advanced students or to handle repetitive drills for those students needing extra work. Increasingly available two-way video links are used to connect teachers and students in remote locations.

The main questions regarding technology in education are summarized in Figure 14.12. Note that nontraditional areas have been faster to adopt the technologies, for example, business training classes—partly to reduce the cost of hiring instructors and partly because the lessons are available to workers at any time and can be studied at whatever speed the student desires.

The Internet is increasingly being pushed as a means to expand the reach of higher education. Several universities offer individual courses over the Internet. The early examples often consisted of simple e-mail-based systems where students worked on their own and occasionally sent messages to the instructor. A few organizations offer complete programs over the Internet. Improving Internet speeds have made new communication methods feasible—including interactive voice and some two-way video communication.

The real key to online education is to use all of the power of the technology to develop entirely new applications. Communication is only one aspect of the Internet. Building more intelligence into the applications to create entirely new procedures will lead to more useful tools. Researchers have worked for years to develop computer-assisted instruction tools that will provide individualized attention to each student. While some individual products have been successful, these tools require considerable creativity and effort to create.

Social Interactions

How does technology affect different areas of society? As any good science fiction book illustrates, advances in technology can alter society in many different ways. Sometimes the responses are hard to predict, and they often occur gradually, so it can be difficult to spot patterns. At the moment, four patterns appear to be important: social group power, equal access to technology, e-mail freedom, and liability and control over data.

Social Group Legitimacy

One interesting feature of technology is that it has substantially lowered communication costs, including the costs of producing and distributing information to large public groups. For example, desktop publishing systems enable groups to create professional-quality documents at low cost. Furthermore, video production facilities are easily affordable by any group, and access to mass markets is provided free through public-access channels on cable television. Web sites can be created by anyone. These technologies enable small groups to reach a wider audience for minimal cost.

The only catch is that with growing professionalism of small-group productions, it becomes harder to distinguish fact from fiction, and it is harder for the public to tell the difference between mainstream, professional commentary and radical extremists. For example, do you believe stories that are printed in *The New York Times*? What about stories printed in supermarket tabloids that sport titles such as “Space Alien Eats Movie Star”? Now consider the Internet and run some searches on medical questions. You will find hundreds of Web sites and comments. Which ones do you believe? Web sites present the strongest challenge

Figure 14.13

A test of cynicism. Which Web site do you believe? Why? Would it help to know that the one on the left is from Johns Hopkins medical center, and the one on the right from a site called arthritiscare.org? With information technology, anyone can create a Web site. It can be difficult to determine the truth. Of course, in many cases, “truth” may be only shades of gray, and there seldom are any “right” answers. All consumers must learn to challenge everything.

ever to trust and reliability issues. Literally anyone can create a site and say anything. Nonsensical comments will be found by the search engines and displayed along with accurate statements. Throw in Twitter and your cynicism meter should go off the scale. Consider the example Web sites in Figure 14.13 and see if you can determine which one to believe.

This issue has some interesting effects. For example, in several instances, disgruntled customers have created sites criticizing companies. If you search for a particular company, you are likely to encounter several of these sites. The Web makes it easy for people to criticize anyone—and the entire world can see the results. Of course, traditional defamation laws still apply, but in situations where there is an element of truth, companies will find it difficult to stop these activities.

The same issues can be applied to television broadcasts, except that for the moment, the high costs of broadcasts restrict this option to a few participants. With his “War of the Worlds” broadcast, Orson Welles shocked many listeners because they had come to accept radio broadcasts as fact. With existing technology, it is possible to create realistic-looking fictional broadcasts. It is not even necessary to resort to tricks such as hidden explosive charges. It is possible to create computer-generated images that exceed the quality of broadcast signals, so they appear to be realistic. Advertisers have made heavy use of these techniques. Every time you watch a commercial, you should remind yourself that a portion of what you are seeing is probably a computer-generated image. Now, imagine what would happen if an extremist organization used this same technology to create newscasts with altered pictures.

Technology Toolbox: Working in a Global Environment

Problem: How do you deal with multiple languages and currencies?

Tools: Foreign currency and language translation tools are available.

Global business presents several challenges. Some, such as cultural issues, are too hard to handle with technology. Others, such as foreign exchange conversion and even some language translation, can be handled by automated systems. However, before you use these systems, you need to understand their features and limitations.

Currency	1 U.S. Dollar Equals
Euro (EUR)	0.69022
Japanese yen (JPY)	80.840
British pound (GBP)	0.62269
Australian dollar (AUD)	0.92384
Mexican peso (MXN)	11.7305

Items sold in one nation are usually priced in the national currency. Products in Europe might be priced in the national currency or in euros. Currencies exchanges are handled by banks or by specialty foreign exchange (FX) brokers. Due to international trade, large banks buy and sell currencies and record the going exchange rates. Currently, the United States uses a floating exchange rate, where the rate changes constantly in response to trade and interest rate differentials. Other nations, such as China or the member European Union countries, fix their exchange rates so that they change only when major economic conditions force a revaluation. Since the rates change, you need to convert currencies on a specific date. The other challenge with exchange rates is that the commonly cited rates are from large interbank transactions. Most people do not get to use those rates and have to pay additional fees to banks or brokers. For example, many credit card transactions use the interbank rates and then tack on 2 percent as a fee. Physically exchanging currencies at a border or airport kiosk will cost you even more in fees.

Oanda is probably the most powerful online FX converter (www.oanda.com/convert). It automatically converts between any two currencies (from 164) on a specified date, using interbank or typical credit card rates. You can use the system to convert prices on your Web site for customers in other countries.

Language translation is another challenge you need to solve to compete in world markets. Ultimately, you need to have Web sites (and product documentation) translated by human experts. However, if you happen to receive a note or see a Web site in a foreign language, or if you simply want to know the meaning of a few words, you can use the automated online translators. Several free translation systems are on the Web. The babel.altavista.com site is one that has been around for several years. Some experimental translation software is becoming good enough that it matches human translators. However, for now you are still better off hiring a person to translate Web sites and documents that will be read by customers. The online sites are useful for quick, approximate translations into your language. In most cases, you should be able to understand the gist of the document, even if it contains errors or poorly worded phrases. An interesting way to test the sites is to enter a phrase in your language (say, English); translate it to a second language (say, Spanish); and then ask the system to translate that phrase back (to English). See how far off it is from the original phrase.

Quick Quiz:

1. What cautionary messages do global Web sites use when converting currencies?
2. If you cannot afford a human translator, is it better to leave your Web site in English, or to use a machine translation?

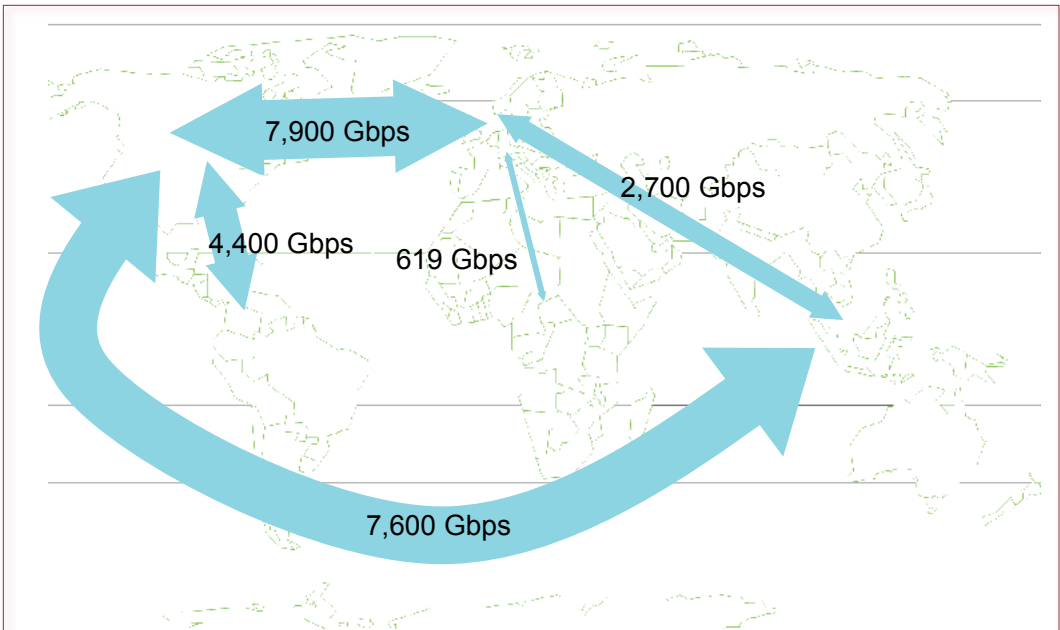


Figure 14.14

International bandwidth. Access to the Internet requires more than computers; it requires high-speed communication lines between nations and continents. As noted by www.telegeography.com, most connections are between the United States and Europe. Numbers are estimates. See/pay TeleGeography.com for better numbers.

Access to Technology

Picture a world in which financial instruments are traded electronically, goods are purchased through computer-television systems, libraries are converted to electronic media, and businesses require suppliers to exchange data over computer links. Large portions of the United States and Europe are getting closer to this scenario every day. Now, what happens to the individuals in poorer nations who can barely afford to eat, much less invest in personal and national information systems? If the means of production are based on technology and certain groups do not have access, the gap between those who have access and those who do not (the **digital divide**) will widen. Although some groups will be content to live without technology, some will become upset at the imbalance.

Figure 14.14 shows that access to the Internet requires more than simple PCs and software. Individuals need access to telecommunication lines. More important, nations need high-bandwidth connections to other nations. The figure shows the currently installed bandwidth between major world regions. Note the major connections between the United States and Europe or Asia, and the relatively small connections to Latin America and Africa. It takes time and money to install new fiber-optic connections across long distances. Telecommunication firms are reluctant to incur these high fixed costs until a region has enough paying customers to cover the costs with long-term usage.

Some companies have worked to give others access to technology. A few recycle older computers to libraries and citizen centers. On the international front, businesses can donate older personal computers to organizations for shipment to

other countries. After three to five years, the technology is often out of date in the United States, but even old technology is better than nothing in some countries. The program “one laptop per child” has attempted to provide low-cost computers to schools in developing nations, but they do not run standard software. And, little work has been done to expand the bandwidth.

Wireless connections offer enormous potential to nations that cannot afford to install fiber-optic connections across their countryside. Wireless is particularly convenient and substantially cheaper to install in high-density areas.

Still, before you begin to believe that the “rest of the world” is poor and bereft of Internet access, consider that several other nations have superior Internet access than the United States. Also, note that even in developing nations, big cities, governments, and universities have computers and Internet connections. These facilities make it possible for most people to obtain access to the Internet—even if they do not have access at home.

e-Mail Freedom

Some organizations have observed an interesting feature when they first replaced paper mail with electronic-mail systems. The first people to use the technology are generally younger, more likely to take risks, and bolder than the typical employee. If the top management levels accept and respond to electronic messages, they are likely to get a different perspective on the organization, its problems, and potential solutions. E-mail systems provide a means for employees (and sometimes customers) at the lower levels to bypass the hierarchy of middle management. A few directed comments and words of encouragement can enhance this effect, which is useful if managers are searching for new approaches to solving problems.

Similarly, customers who spend considerable time on social networks and Twitter can provide useful feedback about your company. Many firms monitor these networks to identify potential problems and provide additional support to highly-connected customers.

Liability and Control of Data

Virtually all of our legal structures and interpretations were created before the advent of a computerized society. Although federal and state governments have passed a few laws specifically to address problems with computer interaction, most legal systems still rely on laws and definitions created for a paper-based world. Sometimes these concepts do not fit well in a computerized environment. For example, how would you classify the operator of a Web site? Is that person a publisher of information, like a newspaper? Or is the operator merely a vendor offering disk space to anonymous writers? In particular, are the owners of Web sites responsible for the content of messages posted on their systems? To date, the court systems have tended to make the decision based on whether the owners exercise “editorial control.” In 1995, the New York supreme court ruled that Prodigy could be sued for libel. An anonymous writer posted a message that was highly critical of the financial status of a certain firm. The firm claimed that the comments were false and sued Prodigy for publishing false information. Since its inception, Prodigy maintained a policy of forbidding people to post “profane” messages. The Prodigy staff used software to scan messages. The court noted that these actions constituted editorial control, so Prodigy could be treated as any other publisher of information (like a newspaper). These concepts were later clarified into law. Now, Web sites that do not exercise control over the content

are merely distribution channels (like booksellers) and cannot be held liable for the content. However, many Web hosting companies place restrictions on content (such as pornography) and will remove a site that is reported to violate its policies.

Government

Can information technology improve governments? Following the expansion of the Internet, the concept of e-government became popular. In some ways, government agencies are similar to businesses. Most federal and state agencies now provide data and communications via the Internet. Some are quite sophisticated.

Government Representatives and Agencies

Governments can be slow to adopt new technologies. Typically, government agencies have limited budgets, long procurement cycles, and requirements for special allocations to acquire new technology. They tend to have smaller IS staffs, who also receive less pay than their counterparts in private business. Moreover, government projects tend to be large and involve thousands of people, which makes them expensive, harder to create, and more difficult to implement.

In the United States, the federal government has moved many data sources to the Internet. Almost all federal data is available in computer form. Many agencies are positioning themselves as providers of economic data to facilitate business decisions. Fedstats ([www/fedstats.gov](http://www.fedstats.gov)) is one of the best starting points for finding data produced by federal agencies. Even municipal governments are beginning to post notices and data on the Internet. Most government agencies are still nervous about electronic commerce. One of the main problems they face is the inability to positively identify consumers over the Internet. Of course, government agencies operate on government time. Little has been done to reduce the time it takes to release government data. For example, data reports from the 2000 census were released over a five-year time period, and data from the 2010 census began slowly trickling out in 2011. Data from many agencies is months or years out of date when it is released. Furthermore, many economic statistics are revised over time, so preliminary numbers you see one month may be replaced with different values several months later. Nonetheless, the government agencies are important sources for many types of data. Government data is important for its accuracy.

Politicians campaigning for office also use technology. But, due to spam, you cannot send direct e-mail to them. Most have Web sites that enable you to enter questions or sign up for marketing spam from the politician's office. For many years government officials have used databases to track letters and comments, solicit contributions, and tailor speeches to specific audiences. Politicians still rely on television to create images, but Web sites are commonly used to provide detailed position papers and background information that is too long to be covered in depth by traditional media.

Politicians significantly use technology in election campaigns. They use databases to pinpoint donors. More aggressively, they use databases to identify voters who will cast votes for a specific candidate, then use reminders and rides to the polls to ensure those voters get to the voting booth.

Democracy and Participation

The U.S. Constitution and its amendments clearly recognize that democracy requires the participation of the citizens. And participation requires that citizens be

- Prevent fraud by voters (identify voters).
- Prevent fraud by counters.
- Prevent fraud by application programmers.
- Prevent fraud by operating system programmers.
- Prevent attacks on servers.
- Prevent attacks on clients.
- Prevent loss of data.
- Provide ability to recount ballots.
- Ensure anonymity of votes.
- Provide access to all voters.
- Prevent denial of service attacks.
- Prevent user interface errors.
- Identify and let voters correct data entry errors.
- Improve on existing 1 in 6,000 to 1 in 10,000 error rates.

Figure 14.15

Electronic voting requirements. Electronic voting sounds convenient and easy to set up—until you look at the detailed requirements. Many avenues for fraud exist. Additionally, complex systems are hard to create and susceptible to errors.

informed—hence the importance of the press. Information is required to produce knowledge, which can lead to wisdom and better decisions. More important, it is not always clear exactly what information will be useful later. The Internet is a powerful source of information. Of course, distinguishing fact from fiction is critical. Yet today it is still possible for a nation to control the content available within its borders. China maintains its hold by owning and controlling all routers that connect to the Internet. Ultimately, it may become impossible for a nation to control all information. Between the massive data flows, encryption, automated document translation, and wireless capabilities, it will become increasingly difficult to control data.

These points were emphasized in the 2011 political upheavals in northern Africa (Tunisia, Egypt, Libya, and so on). Cell phones and the Internet gave citizens the ability to communicate and coordinate their actions. Dictators Mubarak and Gadhafi actually shut down Internet connections and cell phone networks in an attempt to restrict the ability of their citizens to communicate. (Side note to future dictators: It is really hard to convince people you are a benevolent dictator when you take away cell phones and the Internet.) Eventually, people found ways to communicate. In Libya, enterprising workers built a completely separate cell phone network.

Voting

With the fiasco of the 2000 U.S. election, people began to realize the deplorable status of existing voting systems. The level of mistakes due to machine, user, and counter error is unacceptable in a modern society. Several people have mentioned the possibility of creating electronic voting systems to provide faster and more accurate tallies of votes. But many challenges exist as shown in Figure 14.15. Several experts have testified before Congress that they do not believe current technology is capable of surmounting all of the problems. But ultimately, the question comes down to whether a superior system can be developed, even though it may

Reality Bytes: Where Have You Been?

In 2011, researchers looking at cell phones noticed that Apple iPhones and Google Android phones routinely tracked the cell phone location and stored the data in an unprotected file on the phone. Both Apple and Google later admitted that the phones regularly sent the location data to their corporate computers. Both companies apparently used the data to build a location database. Apple and Google are not alone. A Wall Street Journal examination of 101 popular apps found that 47 of them sent location information to app vendors and other companies. Once the data is collected, no rules exist, so it can be sold to anyone else.

Adapted from Julia Angwin and Jennifer Valentino-Devries, “Apple Receives iPhone Location Data,” *The Wall Street Journal*, April 21, 2011.

not be perfect, and whether it can prevent major problems. There is a long history of building and revising voting machines in an attempt to minimize fraud and abuse. But existing machines still miscount an average of one in 6,000 to 10,000 ballots. The other serious drawback to existing systems highlighted in the 2000 election was the usability issue, where thousands of ballots were disqualified and thousands more counted incorrectly because people did not understand them.

A few people have suggested that it would be nice to implement a voting system that works as easily as ATMs or even using their own PCs to connect over the Internet. But electronic voting has two main complications over traditional electronic commerce. First, it is critical to authenticate each voter. Current e-commerce handles this step with credit cards—which are not available to all voters and not secure enough to use as a public voting identifier. (What would stop a business from assuming your identity?) Second, the votes have to be auditable, but anonymous so that no votes can be traced back to an individual. This second condition is even trickier if you are concerned about vote selling. Ideally, voters should not be able to show their final vote to anyone else. If they can, it opens the possibility of buying votes. Currently, there is little incentive to buy votes because there is no way to prove how someone voted, so no way to enforce the agreement.

Voting from your home over the Internet might take years to develop, largely because of the challenge of protecting the client computers and denial of service attacks. Security experts can protect the servers and data transmissions can be protected through encryption. But how can a government ensure the security of a PC in your house? Given the level of viruses, hoaxes, and false statements on Web sites, it would seem to be relatively easy to attack millions of home computers to control an election.

On the other hand, society has an additional critical objective in designing a new voting system: the need to make it easier for people to vote to increase participation rates. To combat this problem, several states have implemented paper-based ballots shipped to each person’s home. Ultimately the point is that no system is perfect, so the question quickly becomes whether an electronic vote system is better than the existing methods, and whether it is possible to prevent significant fraud. In a test of electronic voting systems in the Georgia 2001 election, almost all said the system was easy to use and over 94 percent said the entire state should move to the electronic system.

Reality Bytes: Movie Theaters v. DirecTV

Video is an interesting case in technology. Largely because of the bandwidth issue, video was one of the last entertainment categories to be digitized. It is also hugely expensive to create movies and entire business models evolved to handle the financing, production, and distribution of video, with many of the steps controlled by a few large firms. The one thing that most of the industry agrees on is that movies have a shelf life or immediacy. People will generally pay higher prices for newly released movies, but a considerable amount of back-end money exists for “older” movies that can be sold to a wider audience at lower prices. In 2011, DirecTV signed a deal with some studios that allows the satellite company to rent movies to customers for about \$30—only two months after they debut at the theater. Traditionally, other offerings provided movies four months after release for a price of about \$6. Theater owners and several directors (including James Cameron) expressed displeasure with the plan saying it was a “distribution model that cannibalizes theatrical ticket sales.” Studios counter that most movies make their money within a couple weeks of release and that the need to make up revenue lost to declining DVD sales and changing consumer habits. But director Todd Phillips noted that “Knowing a film will be available at home so quickly removes the sense of urgency people feel to go see the film in theaters.” Directors want to see the large screen and social atmosphere of theaters remain as the primary market for movies. Theater owners are concerned about going out of business. But, ultimately consumers will make the decisions on when they want to see movies and how much they are willing to pay.

Adapted from Michelle Kung and Ethan Smith, “Filmmakers Pan DirecTV Plan,” *The Wall Street Journal*, April 21, 2011.

The issues of electronic voting systems are constantly debated in the press. Computer scientists state that even electronic voting booths can never be trusted, let alone voting over the Internet. Yet, many citizens actually would prefer the convenience of voting over the Internet, so there is pressure to develop a workable solution. Some interesting cryptographic methods exist that have the ability to make it possible. Securely implementing these technologies will take time, and require some interesting adaptations. One powerful trick (homomorphic encryption) is the ability to encrypt votes so that it is possible to record the vote total—without ever observing or decrypting the individual votes.

Information Warfare

As firms and entire economies become more dependent on information systems, the underlying infrastructure becomes critical to the nation. Think about how the information society will work in 10 years or so. Communication, including telephones, will be based on Internet protocols. B2B e-commerce will take place over the Internet, with automated agents placing orders and handling most transactions. Private and government services will be provided through Web sites. Web services will be offered through interlinked sites.

Now, imagine what happens if some nation or group decides to attack this information system. Inexperienced people using software scripts found on various Internet sites have already attacked individual companies. A few major attacks

Reality Bytes: China's State Internet Information Office

China has developed one of the strongest controls over the Internet of any nation. Particularly given the population and size of the Internet, managing and controlling policy can be a complex task. In 2011, China created a new central agency to handle all aspects of the Internet known as the State Internet Information Office. It is not clear how the many existing agencies will fit into the new organization, but it is in charge of “online content management,” supervision of online gaming, video and publications, promotion of news sites, and government propaganda. The Office would also have the authority to investigate and punish people and companies who violate the rules. It will also be in charge of the telecommunications companies that provide Internet access. At least 14 other agencies have a hand in controlling the Internet in China, but the new office makes it clear that the Chinese government will continue to enforce limits on access to the Internet.

Adapted from Michael Wines, “China Establishes New Internet Regulator,” *The New York Times*, May 4, 2011.

have been launched against the Internet DNS infrastructure. These denial-of-service attacks can be mounted by anyone. If an experienced, dedicated group of experts attacked a nation, they could stop service to huge segments of the economy. This threat is one aspect of the Internet that scares many agencies.

The United States and other national defense departments have begun planning for **information warfare (IW)**—in terms of both potential defenses and attacks. The ultimate objective of information warfare is to control the information available to the other side so that you can encourage them to take certain actions. This definition includes the ability to intercept communications, as well as to provide new data that will be accepted as valid. IW goes way beyond hacking into a system or destroying enemy computers and networks. In many ways, IW has been a part of war and conquest for centuries. The increasing use of computers, both in the military and in economies, has made IW more important. IW has existed in many respects from the early centuries of warfare. Some aspects became prominent in World War II, such as code breaking, the Navajo code talkers, the use of the BBC to send coded signals, and misinformation. Misinformation and control of the press (domestic and worldwide) have become key aspects to IW, particularly given the worldwide reach of CNN.

Some U.S. reports indicate that the Chinese military is attempting to develop viruses that can be inserted into foreign networks to disrupt the flow of data or provide false information. In 2010, an interesting virus “Stuxnet” was released on the world. Analysts who studied the virus determined that it was specifically targeted to attack Iranian nuclear facilities and was probably created by some government-funded agency (probably not in the U.S.). Some reports out of Iran indicated that it was successful in causing at least temporary problems at several facilities. Information attacks can be targeted against military or civilian objectives. Military uses of information warfare are common today. One of the first steps the U.S. air force takes is to disable the enemy’s air defense systems to gain control over the enemy airspace.

Civilian attacks are still new, but the potential is huge. The military goal would be to destroy the economic ability of a nation to build and deploy weapons, but an

Reality Bytes: Google v. National India and Kazakhstan

As a leading Internet company, Google encounters many issues around the world. The company has taken the lead in many issues—trying to convince nations to remain open and allow everyone access to content on the Internet. In 2011, Indian regulators passed a set of rules that imposed restrictions on Internet content. Among other things, the regulations created by the Ministry of Communications and Information Technology require Web sites to remove objectionable content and to respond to government requests to remove content within 36 hours. Google was primarily concerned about being held liable for indexing content that was hosted by other sites. But a key issue in any Web site is whether the site is required to monitor posted content to look for possible violations of national laws. In the U.S. the laws do not require monitoring but do require some content to be removed when it is brought to the attention of the Web site publisher. In a more extreme situation, the Kazakhstan government in May 2011 ordered all Kazakh domains (a top-level domain of .kz) to route traffic only to servers in Kazakhstan. Kazakhstan is a former Soviet republic that is governed by a long-term president in an increasingly authoritarian regime. In response, Google suspended operations on its internal Kazakhstan servers and routed all search requests to the generic Google.com servers. Bill Coughran, a Senior Vice President at Google, noted that “We find ourselves in a difficult situation. Creating borders on the Web raises important questions for us, not only about network efficiency but also about user privacy and free expression.”

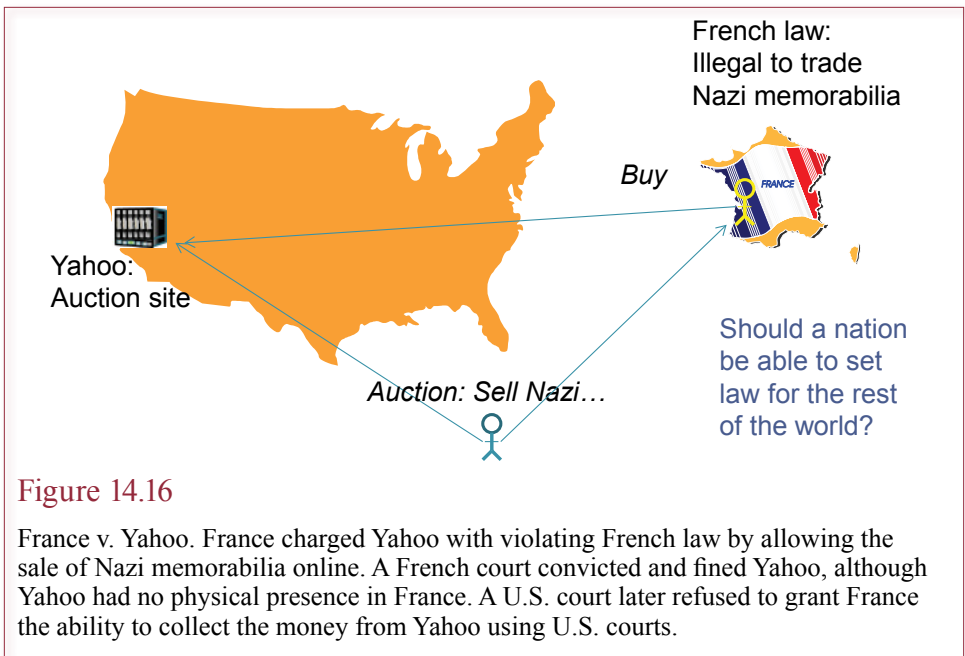
Adapted from Amol Sharma, “Google Raised Objections to Draft India Internet Rules,” *The Wall Street Journal*, May 10, 2011; and Alan Cullison, “Google Redirects Kazakhstan Traffic,” *The Wall Street Journal*, June 8, 2011.

attack would also destroy the underlying infrastructure. The Internet was originally designed to survive military attacks through decentralization and the ability to route around broken links. However, as e-commerce has evolved, several vulnerabilities have been created that would enable governments or terrorists to disrupt major sections of the Internet by attacking some critical points.

In general, the same security controls that businesses use to protect systems on a daily basis are important to defend against international attacks. Ultimately, many aspects of the Internet infrastructure need to be improved to prevent attacks by terrorists, since the underlying components were not designed with security in mind. Several Internet committees are working on these new standards.

Rise of the World-State?

In ancient history (literally), communities of people formed into city-states to share common resources and provide a common defense. Because communication was limited and transportation costs were high, the city-states were largely self-sufficient. However, merchants traveled among cities to barter products that were only available in some locations. Over many years, transportation and communication costs declined, giving rise to nation-states. Through various battles and political arrangements, people accepted the role of the national governments, although some issues are still being fought.



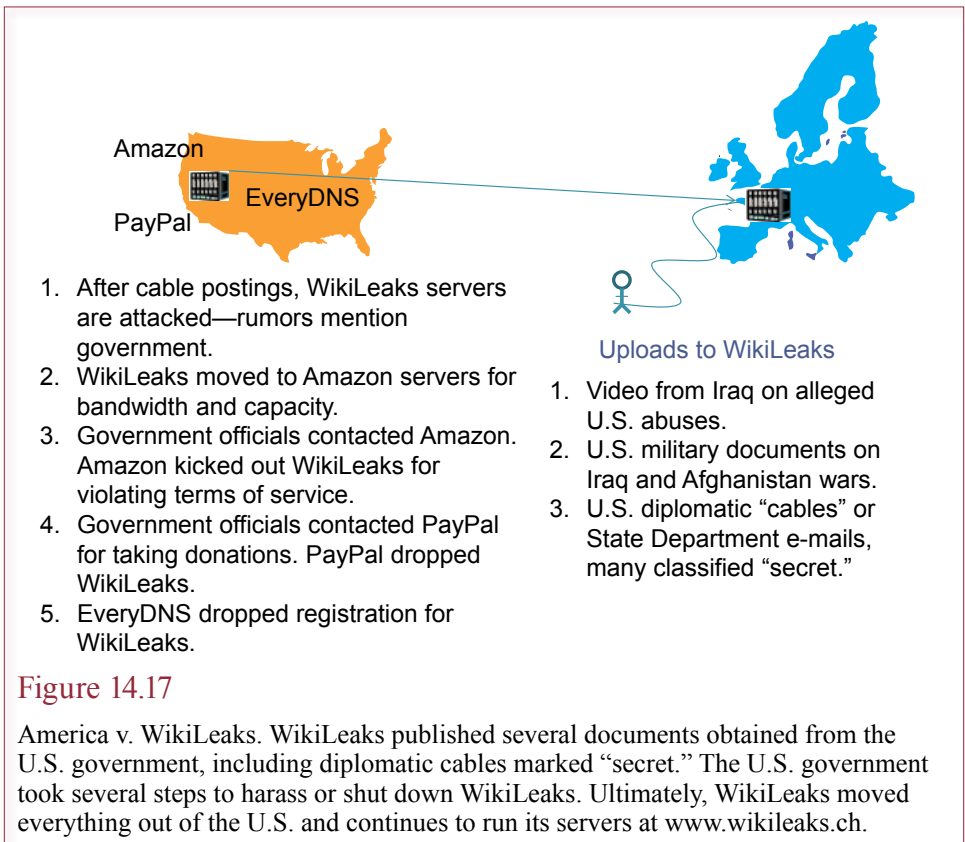
For years, many writers have suggested that increasing international trade, declining transportation costs, and improving global communication will eventually lead to a world-state. National governments might still exist, but commerce would be more regional and global, and world laws would be more important than national policies. The rise of the European Union and other free trade areas (such as NAFTA) are sometimes seen as forerunners of this world.

International e-commerce provides some support for this hypothesis. In an environment where digital data and services can be transferred instantly around the world, it is easy to see the irrelevance of individual national laws. With encryption and a wireless (satellite) connection, how can a national government impose rules or taxes on the digital transfer? If a serious digital monetary system is developed and accepted, how will a nation impose its independent economic policies? Some of these issues are being addressed today by global political organizations. Nations are slowly learning to cooperate and create common procedures and laws.

On the other hand, a world-state would be a massively complex system that would undoubtedly be politically unstable. There are still many regional tensions and periodic fights over physical resources. It would take many years of prosperity and economic growth before nations were willing to accept a truly global government. However, in the meantime, many issues will need to be negotiated in a global setting because they are beyond the control of any national government. Some international organizations facilitate these discussions, but most are somewhat cumbersome.

World Government Cases

Some of the issues in world governments are best seen through cases. Figure 14.16 shows one of the first major international cases. France has a national law that makes it illegal to trade (buy and sell) Nazi memorabilia. Based on their experiences in WWII, this law probably makes sense for France. Yahoo is a U.S.



based company that started as one of the leading search engines. Yahoo also had an online auction system at one time. The problem is that anyone in the world could use the auction system, so someone might offer to sell or buy Nazi trinkets through the system—and conceivably, a French citizen might be the buyer or seller. France apparently asked Yahoo to block all trading in Nazi memorabilia, but Yahoo decided it was too hard or expensive to do that just for France. So, France prosecutors charged and tried Yahoo in French courts for violating their laws. Unsurprisingly, the French prosecutors won—the only surprise is that Yahoo bothered to show up. The courts imposed large fines on Yahoo. However, Yahoo had no physical facilities in France, and later, U.S. courts ruled that France had no authority to use American courts to extract the money from Yahoo. Of course, Yahoo would never be able to establish offices in France in the future without addressing the problems. The real issue of the case is whether one country can impose its laws on other nations, simply because they are connected through the Internet.

Now, consider the case of Microsoft v. Fujian Dongbai Group, which is a department store in China. Microsoft (and the Business Software Alliance) charged the company with violating copyright laws by using copies of Office and Windows on its computers to run its business. In April 2011, Microsoft prevailed and the Chinese company agreed to pay about \$138,000 to Microsoft (see the *Wall Street Journal* note on April 21, 2011). How is this case different from the Yahoo case? The most important difference is that for several years, the U.S. government has diplomatically been pressuring nations, including China, to create

Reality Bytes: Cut Our Network and We'll Bomb You

In 2011, the Pentagon announced that some acts of cyberwar will be treated as any other type of attack on the United States. If electronic attacks on computers or the Internet cause death, damage, or high-level disruptions equivalent to a traditional military attack, then the U.S. will have grounds to treat the attack as an act of war and respond with use of force. Or, as an unidentified military official put it “If you shut down our power grid, maybe we will put a missile down one of your smokestacks.” These new principles are based on the Pentagon’s interpretation of the “Laws of Armed Conflict.” The Pentagon still needs to determine which acts or levels would trigger a response and what level of response might be applicable to each case. And the bigger problem is going to be tracing the actual source of any attack. Still, nations need to begin thinking about and negotiating methods of identifying, stopping, and perhaps retaliating against cyber attacks.

Adapted from Siobhan Gorman and Julian E. Barnes, “Cyber Combat: Act of War,” *The Wall Street Journal*, May 31, 2011.

intellectual property laws (including copyrights). China now has a copyright law, and Microsoft’s case was presented to Chinese courts. So, can a country (the U.S.) impose its laws on other countries? Not directly, but perhaps it can convince others that the law is necessary and each nation can implement similar laws. This situation is a classic case of international cooperation and diplomacy. Over time, several laws have been presented for adoption around the world. Copyright is a big one, but computer crime laws including hacking and anti-terrorism are also important.

Figure 14.17 presents another recent case that is more ambiguous. WikiLeaks is a site and European company that is dedicated to publishing information provided by insiders to reveal corruption or other problems within organizations. In 2010, a person within the U.S. military (possibly Bradley Manning, a network technician), sent three major items to WikiLeaks: (1) Combat video from Iraq showing probable attacks by U.S. soldiers on civilians; (2) Classified government documents regarding the wars in Iraq and Afghanistan; and (3) Thousands of U.S. State Department diplomatic cables (e-mails), many of which were classified as “secret.” This latter group of files appears to have angered President Obama and the U.S. State department. Although some of the documents were simultaneously published by traditional newspapers (such as *The Wall Street Journal*, *The Guardian*, and *El País*), most of the anger appeared to be directed at WikiLeaks. (See news accounts beginning in the Fall of 2010 for many details and rumors.) WikiLeaks quickly fell under attack from people trying to shut down the site with denial of service attacks. WikiLeaks claimed the attacks were coordinated by the U.S. government, but evidence has not been provided to support that claim. To handle the attacks by providing increased bandwidth and server capacity, WikiLeaks purchased space on Amazon’s cloud system. Apparently, U.S. politicians contacted Amazon and asked that the site be removed. Amazon complied immediately—stating that WikiLeaks was in violation of the “terms of service” agreement. Another U.S. based company, EveryDNS, was the DNS registrar for the main WikiLeaks.org name. That company also dropped WikiLeaks as a customer, claiming that the DoS attacks were causing problems with their operations.

This step meant that no one could find WikiLeaks.org by entering just the name. WikiLeaks raised some of its money through donations to a German company that used PayPal to transfer funds. Again, it appears that American politicians pressured PayPal to drop the WikiLeaks company, and PayPal complied immediately. WikiLeaks still survives—in part because a Canadian company (EasyDNS) is handling the domain registration for the WikiLeaks.ch name. But, the case raises important questions about the role of governments in controlling various elements of the Internet. The WikiLeaks case is particularly interesting because it involves the U.S. government and a complete lack of due process or appeal. But, because the firms involved are individual companies, they are free to set their own policies. It is not clear what actions the U.S. government would have taken if companies such as Amazon or PayPal had declined to drop the WikiLeaks sites.

Many subtler international and ethical issues exist across the Internet. For instance, China owns and controls all of the Internet routers in that country. It routinely blocks many sites and has the ability to track online activities of its citizens. As a sovereign nation, China is free to perform all of these tasks. But, some people have criticized American companies such as Google and Cisco for creating tools that enable China to implement these policies. The situation raises the question of whether companies should provide capabilities requested by large customers. A pure business approach would argue that anything that makes more money for the company is good. But, are there features or tools that companies should stay away from? The answer is probably “yes,” but who makes these decisions? Do these decisions need to be made within individual firms, individual nations, or with the help of a global forum? The Internet is still young and many questions remain to be answered.

Crime

Do criminals know how to use computers? Crime has many aspects—both in the Internet/information world and in the “real” world. Security issues related to protecting information systems and Web sites are discussed in detail in Chapter 5. The issues in this chapter refer to questions of how governments can combat crime in society. Criminals today have access to the same technologies as everyone else. Drug dealers and weapons merchants use encrypted spreadsheets to track their sales. Terrorists use encrypted e-mail to transfer information. Con artists use the Internet to steal money from victims. Entirely new forms of harassment and stalking have been created with chat rooms, e-mail, cell phones, and other electronic communication systems. Most people want the government to protect them from these many forms of crime. The complication is that the electronic tools make it more difficult for police to work. So you as a citizen need to identify the trade-offs you are willing to accept.

Police Powers

For years, politicians have used the threat of crime to argue for granting increased powers to police agencies. Interception and decryption of communications (wire-tapping) is a classic example. The United States passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994. It has taken effect and requires that when requested by the government, any telecommunication company must route any communication that passes through its facilities to an off-site U.S. government facility. The FBI similarly created the Carnivore (DCS-10000) system to monitor and record all Internet communications of a targeted person.

Reality Bytes: Do Not Call, We Mean It

Spam, or unwanted commercial messages and phone calls are a global problem. And when most of the phones are mobile and people pay for minutes of usage, the calls are beyond annoying. Most nations have followed the lead of the U.S. and established do-not-call registries. The problem is that many, including the U.S., have minimal enforcement provisions. India, the number two country behind China, in terms of mobile phones learned the problem the hard way. Although a do-not-call registry was established in 2007, it was widely ignored—actually, the list was often used as a base list for calling. Until the Finance Minister Pranab Mukherjee received a telemarketing call while in Parliament in 2010. A new law adds progressively higher fines on telemarketers, and requires commercial messages to be tagged with key numbers or headers. More importantly, the cell phone carriers will be responsible for increasing fines for each infraction; starting at \$2,200 for the first offense and quacking increasing to \$22,000 for the third or more offenses. Wireless carriers are complaining about the cost of installing hardware and software to comply with the law. And the largest provider, Bharti Airtel Ltd, announced it would stop providing text service to telemarketers.

Adapted from Megha Bahree, “India Adds Teeth to Do Not Call,” *The Wall Street Journal*, June 20, 2011.

However, the FBI gave up on its technology and beginning in 2007 now requires all ISPs of any size to purchase and install equipment to collect and forward to a law enforcement agency all transmissions to or from a specific client. VoIP is the primary reason for the law, to enable law enforcement agencies to intercept phone calls placed over the Internet, but it also applies to data. In practice, if you run even a small wireless access point that gives public users access to the Internet, you must install technology to capture these transactions and forward them to the police on demand. On a global scale, the National Security Agency (NSA), in cooperation with other national partners, routinely captures and monitors international communications. Under federal mandate, wireless providers are phasing in locator systems designed to route emergency crews to callers who use cell phones. Of course, these same locator systems could be used by police to monitor the locations of suspected criminals.

Three questions must always be addressed with each new technology: (1) Is the technology effective or are there other ways to accomplish the same result? (2) How can society control the use of the technology and is it worth the loss of privacy? (3) Who is going to pay for the technology? The technology press contains many stories of abuses of power and information—including those by IRS agents and state and local police agencies. The police can also tell stories of how the criminals use modern technology to thwart investigations, and how additional police powers can be used to reduce crime.

Freedom of Speech

As constitutional scholars have long known, freedom of speech is a difficult concept. In practice, many limits are placed on individual speech to protect society. The classic example: you are not allowed to yell “Fire!” in a crowded theater (when there is no fire) because the result is dangerous to many people. Similarly,

there are restrictions on “speech” on the Internet. A big element is that you cannot defame or harass others. While this statement seems obvious, what happens when people sign up with an anonymity server? They could then use free e-mail services, chat rooms, and Web sites to attack other people or companies.

The flip side of this situation is the issue of how to control these problems. Should a police agency have the ability to routinely break the anonymity server to identify all people? But that raises the question of what constitutes defamation and harassment? It is legal for a person to report truthful information about a company or an individual, but sometimes marginal in whistleblower situations. But what if the person being criticized is a public official and uses the police power to retaliate and harass the original person? Of course that action would be illegal as well, but how do you prevent it?

The main thing to remember is that there are many sides to all of these discussions. Also remember that many people have strong personal preferences on each side, and debates are often filled with emotional and unsubstantiated claims. In the coming years, these topics will become increasingly important. It is critical that you form an educated opinion and make sure that your voice is heard.

Gambling

Gambling on the Internet is a multibillion dollar, worldwide business. In many countries, gambling is routine and available at many locations. In the U.S., gambling is largely discouraged—except in some states or cities, and in cases where it is used to raise money for governments, and you can probably find a dozen other exceptions. The Federal Wire Act makes it illegal to gamble by wire. It was originally created to prevent gambling institutions from spreading through telephone and telegraph connections. Each state also has its own gambling laws, making it challenging to determine the status of gambling in any location. However, if it crosses a state line, the Federal law can be applied and enforced. In the early 2000s, the U.S. government used the law to effectively force basic gambling Web sites out of the United States. Of course, several international sites exist and provide gambling to anyone on the Internet. To prevent U.S. citizens from using these sites, The Unlawful Internet Gambling Enforcement Act of 2006 enabled the government to go after credit card companies and banks and prevent Americans from using credit card payments to gamble online. Consequently, it is difficult for Americans to gamble online because it is difficult to make payments and create accounts.

Partly due to the absence of general online gambling, and partly due to the televised national tournaments, online poker became a large business in the United States. At least until April 2011, when the U.S. government shut down several U.S. based poker sites, confiscated their bank accounts, took control of the domain names, and charged several owners of the sites with violating the Federal Wire Act (which includes jail time and monetary penalties if convicted). The initial defense by the owners was that poker is not gambling, but that argument could be difficult to win. However, even if the poker sites return, you should avoid them. By 2011, many poker-bots, or automated systems were capable of beating even the best human poker players. And, if the bots could coordinate their activities within one game, there would be no way to win against them.

The era of online poker playing is probably over. But, how long will it be before something else attempts to take its place? Does the U.S. need a better definition of gambling? Or, should gambling simply be expanded and opened up to any site?

Reality Bytes: Telecommuting Tax Problems

The old world rules that are dependent on physical location cause problems when they encounter new digital technologies. Telecommuting seems like a benefit to employees and businesses. Even for cities, telecommuting should be able to reduce the demands on services such as transportation, highways, and parking. But, as cities face losses in tax revenue, politicians become more creative in seeking ways to make money. In March 2010, the Tax Court of New Jersey ruled that TeleBright Software Corp., a company with its offices in Maryland, was actually “doing business” in New Jersey—simply because one of its employees lived in New Jersey and used telecommunication to work for the firm. Why does anyone care? Because if a company is declared to have a business presence in another state, it also has to pay income and sales taxes on any sales in that state. A survey conducted in April 2011 revealed that 35 states/regions (including D.C and New York City) said telecommuting would create a “nexus” allowing the state to impose income taxes on the company who employs that worker. In other cases, cities (particularly New York City) have declared that telecommuting means the worker is still subject to income taxes at the location of the company. So, a worker living in Kansas and working for a firm in NYC would have to pay income taxes to NYC (and Kansas).

Adapted from Barbara Haislip, “The Hidden Cost of Letting Workers Telecommute,” *The Wall Street Journal*, June 13, 2011.

The evils of gambling are often espoused as a problem, but are U.S. citizens more susceptible to gambling addiction than other nations? Of course, online gambling could be a bigger problem for some people. Money lost online might not seem as real as money lost in hand. Again, these are questions that you have to answer as citizens through voting.

Responsibility and Ethics

How do your actions affect society? Is it possible to follow the laws and still be wrong? In any society, but particularly in one with open information, ethics and morality are important. Laws do not always keep up with changes in society. Think about small towns a century ago. A few basic laws existed, but people generally behaved responsibly, in part because if you gained a negative reputation, people would not trade with you. In an Internet world where people can write almost anything about you for others to find, it is possible that your reputation and honesty will become even more important. For example, eBay uses a ratings system to formalize these concepts. But even without worrying about your future prospects, you should strive to create an honest world.

Users

Computer users have certain responsibilities in terms of computer security and privacy. First, they have an obligation to obey the laws that pertain to computers. The U.S. government and some states, along with other nations, have laws against computer crimes. Most other traditional laws also apply to computer crimes. One law that has received much attention is the copyright law. European and U.S. copyright laws prohibit the copying of software, music, books, movies and other content except for necessary backup. It is the responsibility of users to keep up

with the changes in the laws and to abide by them. In the last few years, publishers have increased their efforts to stop illegal copying of software, called **software piracy**.

Although it might seem to be trivial, making illegal copies of software (or videos, books, or other copyrighted works) can cause several problems. First, it takes money away from the legal owners of the software, which reduces their incentive to create new products. Second, you run the risk of hurting your employer. If employees illegally copy company-purchased software, the owners of the copyright can sue the employer. Third, copying software provides an illegal advantage over your competitors. A small design firm might decide to copy a \$20,000 CAD design system instead of buying it. Consequently, honest firms are hurt because the original firm will be able to make lower bids on jobs because their costs are lower. Fourth, as an individual, you have a reputation to defend. If your friends, colleagues, or employers learn that you are willing to break the law by copying software, they can easily believe that you are willing to break other laws.

Users of computer systems also have an obligation as part of **computer ethics** to customers and clients. Most information in computer databases is confidential. It should not be revealed to anyone except authorized employees. Some nations have laws to protect this privacy. If you find a company violating these laws, it is your responsibility to question the practice.

Users have an obligation to use the information provided by computer applications appropriately. When a user sets up calculations in a spreadsheet, the user must realize that those calculations might be wrong. The calculations must be tested and the information produced should always be checked for reasonableness. You should not believe information solely because it comes from a computer. All data should be verified.

Programmers and Developers

Programmers would never get jobs if they could not be trusted. This trust is one of the most crucial requirements to being a programmer. As a programmer or developer, not only do you have to be honest, but you must also avoid any appearance of dishonesty. For example, practical jokes involving security violations can be dangerous to your career.

Programmers have more responsibilities than many other employees. Software is used in many critical areas. If a programmer attempts a job that is beyond his or her capabilities, crucial errors can be introduced. For example, consider what might happen if an underqualified person took a job programming medical life-support systems. If he or she made a mistake, a person might die. Although mistakes can be made by anyone, they are more likely to arise when a programmer attempts too difficult a job.

Along the same lines, programmers have an obligation to test everything they do. It also means that companies have the responsibility to provide adequate time for programmers to perform the tests. The important step is to identify components that are critical and to build in safeguards.

There have been enormous increases in the demand for software in the last decade. At the same time, new tools allow programmers to create much more complex applications. But our ability to create this new software has far outstripped our ability to ensure that it is error-free. Even commercial programs, such as word processors and spreadsheets, still have errors that can cause problems. In spite of the best efforts of conscientious, talented people, software used appropriately can produce erroneous information.

Liability for erroneous information produced by software has not been fully established yet. Laws and court decisions during the next few years should settle many aspects of who is responsible when software makes mistakes or fails. A related issue is the extent to which the user is responsible for correctly entering information needed by the program and for using the information produced by the program appropriately.

Companies

Every company has obligations to society, customers, employees, and business partners. In terms of society, a firm must obey all relevant laws. For customers, firms must ensure privacy of data. That means companies will collect only the data that they truly need. The data must be safeguarded so that only those who need it for their job have access. If customer information is sold or distributed for other purposes, customers should be notified. Consumers must be allowed to remove their names from any distribution lists.

For employees, a company must provide training and monitoring (compliance programs) to ensure they understand the laws and are following them. Firms must provide sufficient funds to allow the employees to meet their individual responsibilities. Companies must provide enough time and money to test software adequately. Firms have an obligation to allow their employees a certain amount of privacy. For instance, companies have no reason to routinely monitor and read employees' electronic mail messages.

Companies are required to abide by all partnership agreements. In terms of computers, they must safeguard all data acquired from partners. They must not use the data in a manner that would injure the firms involved.

Governments

Federal, state, and local governments have obligations to establish laws that provide a means for those unfairly injured to allow them to gain compensation from those who did the damage. Until the 1980s, relatively few laws at any level were specifically directed at computer usage. Instead, laws intended for other purposes were stretched to cover computer crimes. Frequently, citing mail fraud laws was the only recourse. Some criminals were not convicted because the crime was considered "victimless" by the jury, or the injured corporation declined to prosecute.

Starting in the mid-1980s, the federal government and nearly every state passed new laws concerning computer crime. In 1986, the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act were enacted. The Computer Fraud and Abuse Act makes it a federal crime to alter, copy, view or damage data stored in computers subject to federal law. The law provides fines of up to \$100,000 and up to 20 years in prison. The Computer Abuse Amendments Act of 1994 expanded the original definitions to include transmission of harmful code such as viruses. It distinguishes between actions taken "with reckless disregard" for potential damages (misdemeanor) and intentionally harmful acts (felony). It also modified the language so that crimes causing damages of more than \$1,000 or involving medical records are within federal jurisdiction. Furthermore, it placed controls on states in terms of selling drivers' license records.

Most states have enacted similar laws for the few computers that might not be subject to federal law. European countries have been ahead of the United States in developing legislation to deal with computer crime.

In terms of enforcement, most federal, state, and local agencies have few, if any, officers devoted to solving computer crimes. In fact, many software piracy cases have been pursued by U.S. Secret Service agents. One complication is that most law enforcement agencies lack proper training in computer usage and investigation of computer crimes.

Some Computer-Related Laws

What major laws affect technology and the use of computers?

Laws form the foundation of society. They provide the structure that enables businesses to exist. As society changes, the laws must also be changed. Hence, as the use of computers grows, we can expect to see more laws governing their use. Existing laws will be extended and new ones created. To date, computer laws have been concerned with three primary areas: property rights, privacy, and crime. These areas overlap, and they cannot cover all possible issues. As information technology and robotics become entwined into all our activities, virtually any law can be applied or interpreted to the situation.

Laws continually change and new interpretations and applications regularly arise. You will generally need a lawyer to help you understand and apply the current laws. This short appendix can provide you with only a limited background. You can find additional information in many places on the Web. This information will help you identify problems and generally enable you to obey the laws. However, a lawyer is still the best source of information—particularly if you anticipate problems or conflicts.

Property Rights

A property right gives you ownership and control over an object. While the term originated with physical property, the more important issues now involve intellectual property. If you write a book, a song, or a computer program, you should be able to receive money from sales of that item. Copyright, patent, trademark, and trade secret laws provide definitions of ownership and control transfer of these rights. They provide you with the opportunity to prevent others from using or stealing your work. Each of the four types of property-rights laws applies to different material.

Copyrights are used for books, songs, and computer software. The laws apply to the specific item, such as a book. You cannot copyright a general concept. For example, you can obtain a copyright for a specific word processing application. But other people are free to write similar applications, as long as they do not utilize your specific code or text. Copyrights generally last for 50 years after the death of the writer. In the case of a work produced by a group of workers in a company, the copyright lasts for 75 years after the publication of the work. After that time, the work falls into the public domain, where anyone can use or copy it with no restraints. The times vary by country and have been changed several times, so always check on current values.

Patents were originally designed for mechanical devices, although today you can receive a patent for any device that is innovative and useful. For many years, computer software applications could not receive patents because “laws of nature” including mathematical algorithms were specifically excluded. In the last few years, the U.S. Patent Office has changed this interpretation and now grants patents for computer software. A U.S. patent right exists for 20 years from the date the application was filed. The strength of a patent is that it prevents other peo-

ple from creating a similar product, even if they do not directly copy your work. Consequently, a patent is much more difficult to obtain than a copyright.

Trademarks are used to create a unique name. Once you find and trademark a name (or logo), no one else can use that name without your permission. It is relatively easy to obtain a trademark, except that you must find a name that no one else has already chosen. You can begin your search at the U.S. Patent and Trademark Office: <http://www/uspto.gov>.

Trade secret laws provide you with the ability to seek damages if someone steals your secret information. The catch is that you are responsible for protecting the information. The laws are generally used to enforce a **nondisclosure agreement (NDA)**. If a company wants to work with another company or a consultant, it is a good idea to have the outsiders sign an NDA, in which they agree not to reveal any information you share. If you forget to have them sign an NDA and they release your “secret” information, you will have few options. It is your responsibility to protect the data.

These four basic protections have different purposes and different strengths and weaknesses. Copyrights and trademarks are relatively easy and inexpensive to obtain. You simply fill out a form, submit the material, pay a fee, and wait a few months for the agency to process the request. Actually, a copyright exists as soon as you create the material. You do not need to file the registration form. However, there are some legal and monetary advantages to registering the copyright. Patents require considerable documentation and a formal review to identify prior and related patents and to determine the legitimacy of the innovation. They usually require the help of a specialized law firm, take at least a year to obtain, and will probably cost about \$30,000 in legal and processing fees. Trade secret protection requires no registration with the government, but requires you to create and enforce a security policy to ensure that your information is adequately protected.

In a digital age, copyright law is the most challenging to apply and to enforce. The first question is identifying ownership. Who owns a particular item? If you write a book on your own time with your own resources, then generally you own the rights. If you write a computer program for your employer as part of your job, the employer owns the copyright. Interestingly, if you are an outside contractor and create a program for a company, it is more likely that you own the copyright, unless you agree to transfer the rights.

There is an interesting exception to copyright law: mere collections of data cannot be copyrighted. Consider the example of *Feist Publications v. Rural Telephone Service* [499 U.S. 340 (1991)]. Feist wanted to publish a telephone directory, but Rural would not provide the data. So Feist copied much of the data from Rural’s printed directory. The U.S. Supreme Court eventually ruled that Feist’s action was not a copyright infringement because the directory contained only data, which is not sufficiently original to obtain a copyright. Now consider the case of *ProCD, Inc. v. Zeidenberg* [86 F3d 1447 (7th Cir. 1996)]. ProCD collected and published a CD-based list of phone numbers and addresses, which they generally obtained from printed phone directories. Zeidenberg purchased a copy of the CDs and transferred them to his Web site. He then charged people to access the site. ProCD sued for violating the copyright laws. Based on the Feist case, Zeidenberg was found innocent of copyright infringement. However, he was guilty of violating the shrink-wrap license agreement that came with the CDs. Note that the data collection argument probably applies to most data collected by federal and state agencies.

Copyright protection gives you the ability to stop others from profiting from your work. There are a few minor exceptions—such as parody, excerpting short quotations, and educational “fair use,” which allows educational institutions very limited provisions to make a limited number of copies for teaching purposes. A more interesting, unanticipated exception involves money. Consider the 1994 case of *U.S. v. LaMacchia*, who was a student running a bulletin board system on university computers. He routinely placed commercial software on the site and allowed people to download (steal) the software for their own use. The catch is that he did not charge access to the system and made no money from the process. Without this profit motive, the court ruled that LaMacchia could not be convicted on charges of criminal violation of the copyright laws. Of course, the commercial software vendors could sue him on civil grounds, but unless he was an unusually wealthy student, there would be little gain. On the other hand, the university could throw him out for violating university policy. Congress has modified the copyright provisions to cover this situation, so now anyone who violates copyright laws can be criminally charged, fined, and potentially jailed.

Copying becomes a more serious problem every day. As more works are created and distributed in digital form, it becomes more difficult to protect them. Even though you might have a legal right to prevent copying, it becomes increasingly difficult to prevent the distribution of your work, particularly if individual ethics are weak. For example, say that you write a story and sell it through your Web site. Once the first few people have read the story, they could copy it and e-mail it to their friends. What are you going to do? Arrest and sue your customers who first read the story? On the other hand, if a publisher took your story, printed it, and sold it, you clearly have the legal authority and monetary incentive to seek compensation. Consider a similar example. You build a Web site and create some interesting graphics and sound effects. Over time, other people routinely download your objects and use them on their own sites. Have they violated copyright laws? Can you stop them? Can you even find them? Would it be economically worthwhile to pursue them?

It is unlikely that individual motivations and ethics will improve. That is, despite the laws, many people will still copy anything they can (software, art, text, photos, video clips, and so on). Whatever technology might be applied, it is unlikely to be economically feasible to pursue them. Yet without incentive, why should you create and distribute new works? One possible outcome is that large, expensive content will disappear. Why should you write and distribute an entire book in one piece, when most people would steal it instead of paying \$20 a copy? Instead, you could sell the book a section at a time, for a few cents per section. By releasing the sections over time, people would have to pay to receive the most recent (and organized) sections. Yes, some people might wait and have a friend pay for the section and e-mail it, but it is a question of economics. If the price is low enough, more people will opt to get the data earlier and directly from the source.

The federal white paper (“Intellectual Property and the National Information Infrastructure”) contains an extended discussion of copyright issues and possible federal solutions. It is available online from the Information Infrastructure Task Force (IITF) Web site. You should also read Pamela Samuelson’s criticism of the white paper proposal, which points out that the discussion strongly favors copyright holders as opposed to the public, particularly since the primary author (Bruce Lehman) was a lobbyist for the copyright industry.

- Freedom of Information Act
- Family Educational Rights and Privacy Act
- Fair Credit Reporting Act
- Privacy Act of 1974
- Privacy Protection Act of 1980
- Electronic Communications Privacy Act of 1986
- Video Privacy Act of 1988
- Driver's Privacy Protection Act of 1994
- Communications Assistance for Law Enforcement Act of 1994
- Health Insurance Portability and Accountability Act of 1996
- Children's Online Privacy Protection Act of 1998
- Identity Theft and Assumption Deterrence Act of 1998
- Graham-Leach-Bliley Act of 1999
- U.S. Patriot Act (antiterrorism) of 2001
- CAN-SPAM Act of 2003
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)

Figure 14.18

Privacy laws. Only a few specialized laws exist to protect privacy in the United States. Some, like the Patriot Act, have actually removed earlier privacy protections.

Privacy

Privacy is an intriguing concept. Humans are a social group: we can accomplish far more by living in communities and sharing our talents. Yet individuals have a desire to keep some things private. More to the point, we have a desire to control what information we wish to share. For example, you might not want everyone to know exactly how old you are or how many times you were sick last year, but it is okay if your mother knows these things, and possibly essential that your doctor knows them.

Society has a vested interest in knowing some things about you and your life. For example, communities need to know how much you paid for your car and your house so they can fairly assess taxes. Society needs to track criminal behavior to help identify antisocial people who might harm others. Medical researchers need to track diseases to identify trends, causes, and potential solutions.

Businesses have an incentive to obtain considerable amounts of data on groups and individuals. And individuals have an incentive to provide some information to businesses. Whenever you make a purchase, you need information, and businesses are generally happy to provide you that information. The problem is how do you find the business or company that best matches your needs? Conversely, how can a company identify its potential customers? With no information, companies might resort to mass e-mail (spam) that clogs networks and irritates people who have no use for the services advertised.

The catch is that we do need to share information about ourselves, with government agencies, with researchers in various disciplines, and with businesses. Yet there is no reason that everyone in the world should be able to obtain every detail of our lives. The difficulty lies in determining where to draw this line. It is

further complicated by the fact that every person (and social group) has different preferences.

First, it is important to realize that there is no constitutionally defined “right to privacy,” especially with respect to data. A couple of Supreme Court rules have interpreted a right to privacy within the constitutional freedoms. But these rights apply only to governmental intrusion. A few laws have been enacted in the United States to provide minimal restrictions on the use and sharing of personal data. Figure 14.18 lists the most notable laws. Most are related to financial data and credit reporting agencies.

The Freedom of Information Act generally provides people with the ability to obtain information held by governmental agencies. There are limits for national security and on the release of data relating to individual personal data. For example, you cannot ask the IRS for personal information about your neighbor.

The most important feature of the Family Educational Rights and Privacy Act is that it limits the release of educational data. Institutions can release basic information such as the names of students (commonly sold to businesses), but they cannot release grades without the students’ express written permission.

The primary purpose of the Electronic Communications Privacy Act was to extend traditional wiretap provisions to “electronic communication,” which includes cellular phone and e-mail transmissions. Essentially, the law makes it illegal for individuals to intercept these conversations, and requires law enforcement agencies to obtain court permission to intercept and record the conversations. On the other hand, it is specifically legal for an individual to record his or her transmissions (although a few states limit this right). Consequently, employers generally have the legal right (since they own the equipment) to monitor most communications by employees. Note that there may be some exceptions and an honest employer will always notify employees first.

The Fair Credit Reporting Act primarily gives consumers the right to inspect credit records—and it gives them the right to correct errors. The Driver’s Privacy Act limits the use and release of state motor vehicle data. Its primary purpose was to prevent release of specific data to individual requesters. However, it has generous exceptions for insurance companies, research, and business use. The Video Privacy Act was created to limit the release of rental records from video stores and libraries.

The Privacy Protection Act of 1980 is primarily concerned with law enforcement investigations. It provides some definitions for when police searches are legitimate and when they are an invasion of privacy. The act predates the advances in information technology, so it is generally silent on the issue of privacy in terms of electronic data.

On the other hand, the Privacy Act of 1974 deals more directly with the collection and dissemination of information by the federal government. It specifically limits the collection of data by an agency to information that is relevant to its work. It provides citizens with the ability to examine and contest the data. The act initially limited agencies from sharing and matching data with other agencies, but most of these restraints have been removed by subsequent amendments. For example, the postal service is generally not permitted to disclose data on individual addresses. However, it does release data to a few large commercial service bureaus. Companies can submit address lists to these bureaus for correction of their mailing lists.

The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunications firms to pay for wiretap facilities for police to listen to conversations. In 2004, the FTC began discussions to expand the coverage to nontraditional communication providers, such as ISPs.

The Health Insurance Portability and Accountability Act (HIPAA) is used to limit sharing of medical information. Many health care organizations now ask you to sign forms that give them the authorization to share the data. Since it is unlikely that consumers have the ability to refuse to sign or modify these preprinted agreements, the overall effectiveness is minimal.

The Children's Online Privacy Protection Act is much stronger, and if you run a Web site, you need to be aware of its provisions. As long as you make it clear that you are collecting data only from adults, the law does not apply. However, if you do collect data from children, you must be careful to minimize the personal data collected and generally have to obtain "verifiable parental consent."

The 1998 Identity Theft and Assumption Deterrence Act prohibits "knowingly transfer[ring] or use[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." That is, it specifically makes identity-theft illegal, and targets the person who steals the identity, even if that person does not use the stolen identity.

The Graham-Leach-Bliley Act of 1999 primarily deregulated some financial services. In exchange, it imposed some trivial privacy clauses. In particular, it requires financial institutions to notify customers that they have the right to opt out of (1) selling their names to other companies and (2) marketing requests from the institution. Institutions reportedly spent hundreds of millions of dollars sending notices to customers, but many feel they deliberately made the process obscure and few consumers replied to the mass mailings. Consequently, businesses are basically free to continue using consumer data in any manner they want.

The U.S. Patriot Act was not directly concerned with privacy. However, it effectively repeals almost all governmental restraints. Someday it might result in some interesting lawsuits. One objective was to remove restraints to federal sharing of data.

The CAN-SPAM Act is a halfhearted attempt to reduce the fraud involved with most unsolicited commercial e-mail (spam). Although it is a relatively weak law, you need to make sure that your messages conform to its provisions. For example, you need to include a physical address in each unsolicited message. The message must state that it is an advertisement. You cannot include false return addresses or message headers. And you must provide a working opt-out system. It also imposes limits on how you collect e-mail addresses. Individuals cannot sue violators, but ISPs do have the authority to sue for substantial sums of money. The most powerful aspect of the law is that it applies to the sender of the message and to the firm being advertised. To be safe, if you send unsolicited e-mail messages, be sure to send them yourself from a verified list. Do not purchase lists, and do not use third parties to send messages on your behalf.

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) primarily added definitions and a few features to the Fair Credit Reporting Act. A couple of useful points from the FACTA of 2003 is that credit agencies must provide free copies of credit reports to customers once a year (<http://www.annualcreditreport>).

com), and that merchant receipts cannot contain more than the last five digits of a customer's credit card number.

The bottom line is that this piecemeal approach to privacy means that it is difficult for consumers to determine their rights and for businesses to identify their responsibilities. Consequently, except for the few specific limitations (e.g., credit and educational records), most businesses are free to collect and share information. On the other hand, you can improve relationships with customers by always asking them for permission to use and share personal data. Keep in mind that states have their own laws that apply to transactions and companies within that state. For example, California prohibits merchants from requiring personal information from customers when they make a purchase. An interesting decision in 2011 pointed out that even asking for the customer's ZIP code—a common marketing practice—was in violation of the state law.

Information Era Crimes

As commerce moves to digital form, existing crime laws need to be extended and new ones need to be created. The biggest concerns are fraud, theft, and destruction of property. To understand the complications, consider what happens if someone steals your car. Why is that bad? Largely because you no longer have the use of the car. Now, what if someone steals your company's marketing plan? Why is that bad? You still have the use of the plan. Similarly, what if someone deleted your computerized customer database? Assuming that you are smart enough to keep a backup, what have you lost? The point of these questions is to show you that our traditional views on crime might not apply to crime related to information. Furthermore, computers create the prospect of new types of crime. For instance, what happens if someone writes a program that prevents you from obtaining access to your financial records? The alleged criminal did not steal or destroy anything, so what crime has been committed?

The Computer Fraud and Abuse Act of 1986 provides answers to many of the questions regarding crime in the digital realm. In particular, it outlaws (1) access to computers without authorization; (2) damage to computers, networks, data, and so on; (3) actions that lead to denial of service; and (4) interference with medical care. Interestingly, the act charged the U.S. Secret Service with enforcement.

Enforcement of the act has been challenging. It has been difficult to find qualified law enforcement personnel, including prosecutors. Besides, many businesses are reluctant to prosecute cases because they do not want competitors or shareholders to learn the details. On the other hand, sometimes companies and the Secret Service are too enthusiastic in their pursuit of alleged criminals. For example, one of the first cases supported by the Electronic Frontier Foundation (EFF) involved a (bulletin board system) BBS that supplied a document obtained from the telephone company that detailed information about the 911 system. The phone company complained that the document was stolen and that hackers might use it to break into its system. The Secret Service confiscated the BBS computer equipment and arrested the teenage owner. In court, with the help of the EFF, it was shown that the document could be purchased from the phone company for a few dollars.

Examining crime historically, the same problems exist in preventing more traditional crime and enforcing the laws. In the United States, it was the introduction of the FBI and their professional investigative techniques that improved the detection and enforcement of various crimes. In the digital arena, until society

gains more experience and improved training of police, attorneys, and judges, it will face the same problems of weak laws, difficulty in prosecution, and variable enforcement.

The Digital Millennium Copyright Act (DMCA) of 1998 changed some copyright provisions to synchronize the U.S. laws with the European laws. It also included a unique controversial provision that makes it a federal crime to create or to distribute devices that circumvent copy protection schemes. Part of its original purpose was to prevent people from advertising and selling black boxes to decode scrambled satellite TV signals. Many people believe that these provisions are too strict and that they infringe on the free speech rights in the Constitution. For instance, some researchers have been threatened with prosecution under the DMCA if they attempted to publish their work. The problem with copyright laws is that they can provide only limited legal protection. To enforce these laws, a copyright holder generally has to prosecute violators. But as the record industry was aware in the Napster case, it is virtually impossible to find everyone who copies a song—even more impossible to take them all to court. So, property owners are searching for ways to prevent casual theft. The problem is that in theory, it is impossible to completely prevent the copying of a digital work. So, portions of the DMCA are required to make it difficult for people to sell circumvention technology. By making it more difficult for people to copy a work, the laws essentially raise the cost of stealing. But there are fine lines between protecting copyright holders, protecting consumers' rights to use a work, and protecting everyone's right to study new ideas. It will take time and discussion to draw these lines.

Driven by the September 11 attack on the World Trade Center in New York, the U.S.A. Patriot Act (antiterrorism bill) of 2001 provides considerable new powers to federal, state, and local police agencies. Some of these provisions reduce privacy by making it easier for police agencies to monitor conversations, intercept e-mail and Internet messages, and detain people without cause. Law enforcement agencies are asking for even more flexibility to investigate people. These provisions do have some justifiable uses, and there are times when enforcement agencies have to jump through too many hoops to perform their jobs effectively. However, as J. Edgar Hoover proved, the challenge lies in preventing abuse of the laws, particularly preventing people from using them as political tools.

Cloud Computing

What risks are created through using cloud computing? Cloud computing raises some interesting questions—particularly from a legal perspective. A private cloud—owned and operated by your own company in one or two locations is less of an issue. As long as you control the location and operation of the servers, a private cloud is no different from any other set of servers. The problems begin to arise with public clouds—when you rent processors and data storage space on servers run by other companies. Three basic problems arise with storing data and processing public clouds: (1) Data is transferred across multiple national boundaries and subject to laws in multiple nations; (2) Shared servers might be at risk if police confiscate or search the computers because of a second company, or if attackers initiate a denial of service attack against another company on the server; (3) With multiple levels of contractors and subcontractors, you must ensure everyone respects the security and privacy of your data.

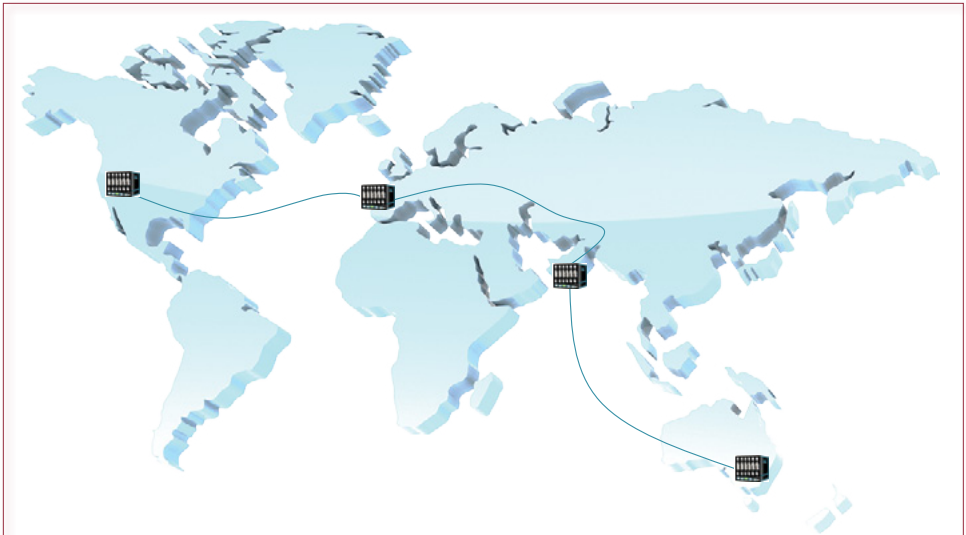


Figure 14.19

National location issues in the cloud. If your data is transferred across multiple borders and stored in multiple countries. What national rules need to be followed? What countries might seek to control or limit your use of the data?

Data in Multiple Countries

Figure 14.19 shows the first issue. One of the strengths of cloud computing is that multiple servers in different locations are used to hold the data—both as backup and to provide faster access across the world. These are useful technical attributes. But, from society's perspective, the data is crossing multiple boundaries and is potentially subject to laws in multiple nations. For instance, what if some of the customer data is transferred to servers in Europe? Does that data become subject to European privacy laws—which are much stricter than those in the United States? But, do you even know where the data is currently stored? What if you are storing data that is politically sensitive? Can one nation confiscate or block your data?

These questions are not hypothetical. In 2010, the Web site WikiLeaks (not a U.S. company) began releasing data that it obtained from sensitive U.S. diplomatic e-mails. The U.S. government was unhappy about the release of the data—which they claimed was stolen (and then given to WikiLeaks). At one point, the WikiLeaks servers were subjected to a distributed denial of service attack and they struggled to remain online. The company paid Amazon to host their content on the Amazon cloud servers—with the hope that the huge bandwidth and distributed service would mitigate the effect of the attacks. Technically, the process worked. But, high-level politicians in the U.S. government contacted Amazon (a U.S. company) and urged them to stop hosting WikiLeaks content. Amazon complied and removed the content. The U.S. government also pressured the U.S. company that was providing DNS services to WikiLeaks and told them to drop the listing—so no one could go directly to the Web site. The WikiLeaks site is currently available through a Swiss registration: www.wikileaks.ch. (This information is available in many news reports from late 2010 and early 2011.) Regardless of which side you might take in the WikiLeaks discussion, the business point is that national gov-

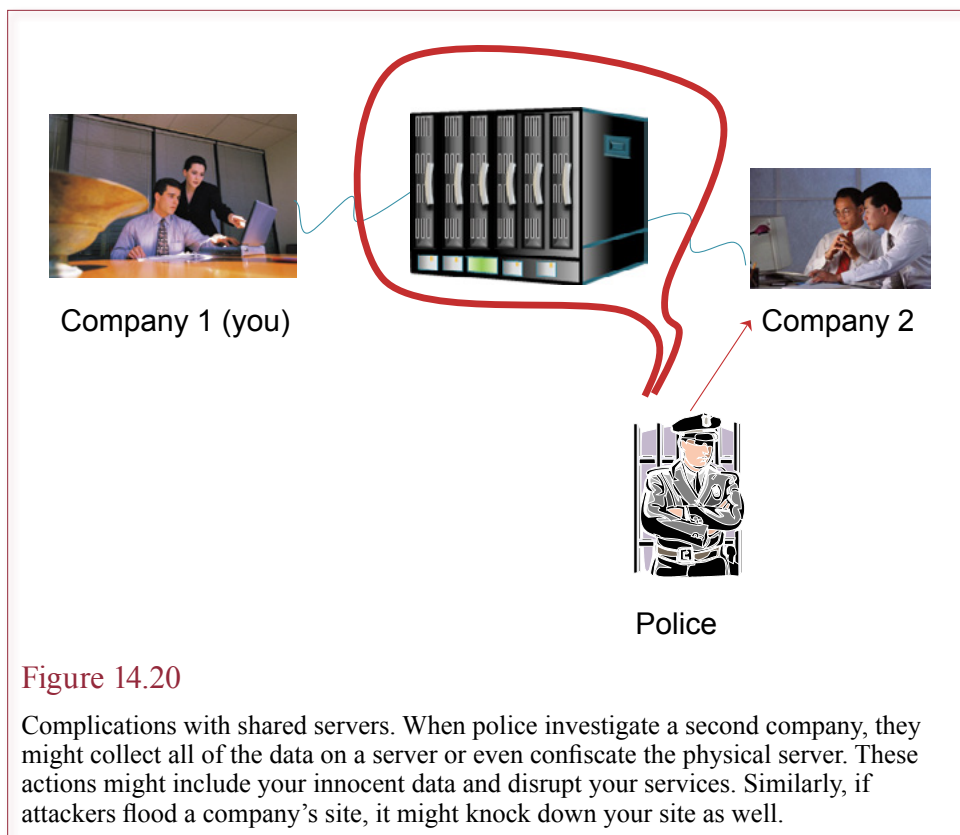


Figure 14.20

Complications with shared servers. When police investigate a second company, they might collect all of the data on a server or even confiscate the physical server. These actions might include your innocent data and disrupt your services. Similarly, if attackers flood a company's site, it might knock down your site as well.

ernments can exert huge control over cloud service providers—depending on the location. Political, security, and tax issues could vary depending on the location of your data. So, you might have to write contracts to control exactly where the cloud provider will store your data. However, in a related situation, Research in Motion, the Canadian company that sells the Blackberry cell phone and service encountered problems in 2010 and 2011. Several nations insisted that the company run e-mail servers within their countries—so national investigators could confiscate or tap the servers if necessary to control communications by citizens within their countries.

If you want some idea of government involvement or interference in the Internet, check out Google's statistics (<http://www.google.com/transparencyreport/governmentrequests/>). Interestingly, the United States and Brazil are at the top of the list for countries asking Google for data and for requests to remove links. In 2011, Freedom House also examined national limits placed on Web traffic and digital media (Sanja Kelly and Sarah Cook, *Freedom on the Net* 2011).

Threats to Shared Servers

As shown in Figure 14.20, a second potential problem with cloud computing is that the servers and Internet connections are ultimately shared with other companies. The cloud provider makes money by building huge server farms and then leasing out capacity to many customers. In many cases, the companies lease virtual machines, and any physical server can run many virtual machines.

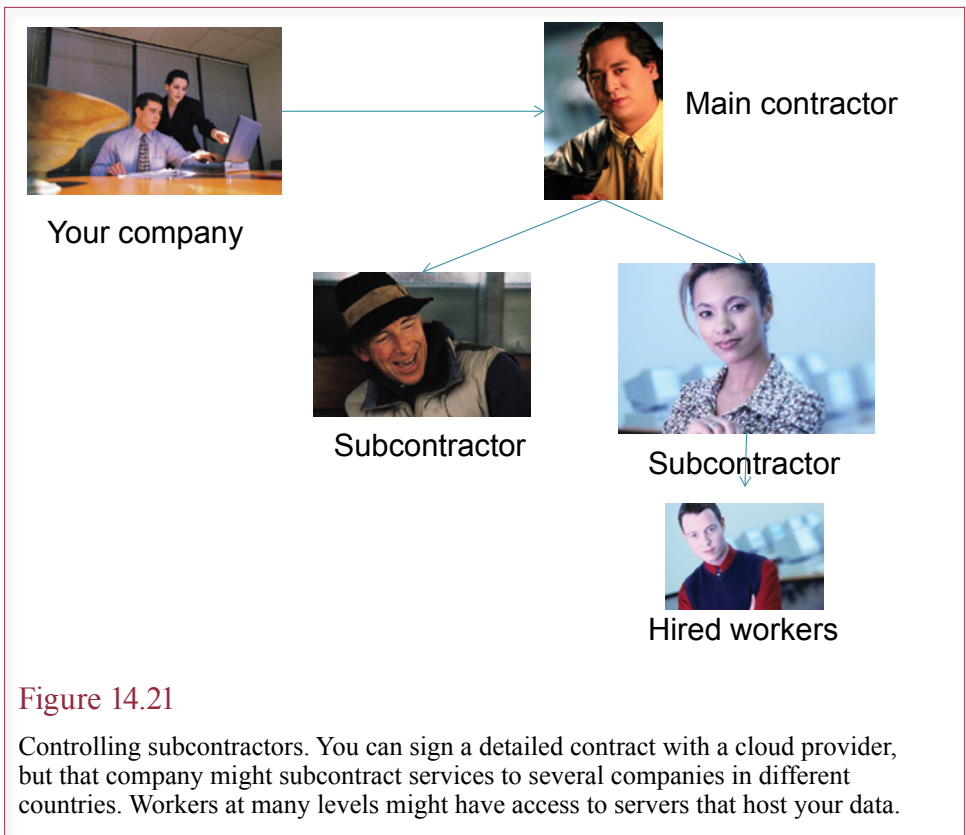


Figure 14.21

Controlling subcontractors. You can sign a detailed contract with a cloud provider, but that company might subcontract services to several companies in different countries. Workers at many levels might have access to servers that host your data.

The problem with sharing the physical machine is that it is not always easy to separate the companies. At least a few cases have already arisen where police investigators have confiscated entire physical servers to gather evidence against a company using the server. The problem is that taking down the entire server affects other companies. Even if the police only need to collect data, they are likely to collect all of the data—including yours. Similarly, an attacker or group of people might become upset at a particular company and launch a denial of service attack against that company. If that company uses the same cloud service as you do, it is likely that your server and Internet connection will be disrupted as well. Stronger cloud providers like Amazon might have enough bandwidth and server capacity to handle the increased load, but it is still a potential risk.

Subcontractors

Figure 14.21 shows a more subtle problem with cloud computing services. When you sign a contract with a cloud service provider, you deal with the top level, but many sublevels can exist below that one. For example, it is possible that each server location is run by a separate contractor. Employees from several contractors might have access to the servers, and ultimately the data, at any location. For instance, network and security specialists, database administrators, and server operators might all be hired by different companies. Throw in electricians, cleaning companies, and security guards and multiply by the number of countries where the servers are located. Potentially dozens of companies might have access

to the physical computers and data in different locations. Hopefully, all of them are trained and honest and know how to protect your data. But, what if you are required to guarantee that the data is accurate and protected? For example, you might want to store employee or healthcare data. Realistically, can you meet that guarantee when you do not know all of the levels of people who might have access? Encryption might help, but only if the encryption keys and all decryption are handled by local servers.

For most cases, it is possible to handle these three types of problems, so they are not intended to suggest cloud computing should be avoided. Cloud computing can provide some significant benefits. But, you need to be aware of these potential problems before you commit to a cloud service provider so you can ask the right questions.

Summary

Technological change and increasingly aggressive use of information systems by businesses have several consequences. Technology affects individuals, their jobs, educational systems, governments, and society as a whole. Businesses have to be careful to protect the privacy of consumers and workers. Security provisions, disclosure policies, and audits are used to ensure that data is used only for authorized purposes. To ensure accuracy, it is crucial to allow customers (and workers) to examine relevant data and make changes.

Technology is generally believed to increase the total number of jobs available. However, the workers displaced by the introduction of technology are rarely qualified for the new jobs. Businesses and governments need to provide retraining and relocation to help those workers who lose their jobs. Sometimes technology allows physically disabled people to work in jobs they might not otherwise be able to perform.

Improved communication networks, huge databases, and multimedia tools provide possibilities for education and training in the public and business sectors. However, because of high development costs, technology tends to be used for specialized training.

Governments have long been involved in data collection, and technology enables them to work more efficiently. Of course, many political observers would argue that perhaps governments should not be *too* efficient. For example, it would be difficult for businesses to operate in an environment where the laws were changed every day. Technology also has the potential to improve communication between citizens and their representatives.

Technology and society produce other interactions. One feature is that lower prices, improved capabilities, and ease of use have made improved communication available to virtually any size group—providing a wider audience for small extremist groups. The new technologies also offer the ability to alter pictures, sound, and video, making it difficult to determine the difference between fact and fiction. Another important social issue is providing access to technology for everyone. It would be easy to create a world or nation consisting of *haves* and *have-nots* in terms of access to information. Those with information would be able to grow and earn more money, while those lacking the data continually lose ground.

Increasing dependence on technology brings with it new threats to the security of the firm. Managers need to recognize and evaluate these threats and understand some of the techniques used to minimize them. The most common threats come from inside the company, in terms of workers, consultants, and business partner-

ships. These threats are difficult to control, because firms have to trust these individuals to do their jobs. Training, oversight, audits, and separation of duties are common means to minimize threats. Depending on the communication systems used, there are threats from outsiders and viruses that can access computers with modems, over networks, or by intercepting communications. Dial-back modems, access controls, encryption, and antivirus software are common techniques to combat these threats.

Working in today's business environment means more than just doing your job. Each individual and firm has ethical obligations to consumers, workers, other companies, and society. In addition to obeying the laws, it is important for workers and companies to remember that the data in information systems refers to real people. The lives of people can be adversely affected by inaccurate data, poorly designed information systems, or abuse of the information.

A Manager's View

As a manager, you need to understand how businesses, technology, and society interact. Dealing with changes in privacy and security threats will become increasingly important to managing a company. Evaluating changes in society will also give you an advantage in the marketplace; it is important to know your customers. As a citizen, you need to be aware of the negative and positive effects of technology. In particular, changes in technology often lead to changes in political power and control. As a manager and a citizen, you are obligated to make ethical decisions and to understand the consequences of your actions.

Key Words

computer ethics
cookies
copyright
digital divide
digital rights management (DRM)
high-bandwidth digital content protection (HDCP)


information warfare (IW)
intellectual property (IP)
nondisclosure agreement (NDA)
patent
privacy
software piracy

Web Site References



	Technology and Society	
ACM/society		www.acm.org/usacm
Center for democracy and technology		www.cdt.org
Center for information technology and society		www.cits.ucsb.edu
Computer professionals for Social Responsibility		www.cpsr.org
Internet Society		www.isoc.org
	Privacy	
Electronic Frontier Foundation		www.eff.com
Electronic Privacy Information Center		www.epic.org
FTC advisory committee		www.ftc.gov/acoas
FTC privacy and security		business.ftc.gov/privacy-and-security
Platform for privacy preferences		www.w3.org/P3P
Privacy, ACM		www.acm.org/usacm/privacy
Privacy International		www.privacyinternational.org
Privacy Rights		www.privacyrights.org

Review Questions

- ✓ 1. Do employees need to worry about the data collected by their employers?
2. If everyone is identified by some biometric measure, will that cause more dehumanization? Will it reduce individual privacy?
- ✓ 3. Do you think increasing use of computers causes a loss of jobs? What about in the past or in the future?
4. What are the personal benefits to telecommuting? Why would people choose to return to commuting jobs after trying telecommuting?
5. Do computers and digital content change the balance of power relationship between consumers and businesses? Should consumers have a right to make personal (backup) copies of digital works?
6. How does information technology add legitimacy to fringe groups?
7. Do you think state, local, and federal governments are making efficient use of computers? Will citizens ever be able to vote online?
8. In what ways have computers affected society and organizations? Will these patterns continue? Are there other important patterns that might arise?
9. Should governments be granted more powers to monitor and investigate people and transactions on the Internet?
10. What are the ethical responsibilities of users in terms of information systems?

11. Do we need additional privacy laws in the United States? What provisions would you add?
12. As a business manager running a Web-based company, which laws and rules do you need to pay careful attention to?
-  13. What is information warfare and what controls or oversight should be placed on it?
14. List the primary U.S. laws related to computer crime and describe each in one sentence.
15. If data is stored in an international Web cloud, what potential problems exist for companies? Do we need new world laws to cover these situations?
16. If you write a blog and publish it on a Web site, who owns it? Can other users copy it? What if you are paid by your company to write the blog?
17. Should governments have teams to create computer viruses that can be sent to other countries?

Exercises

-  1. Research the tools (hardware and software) available for a new employee of yours who is blind. List the sources, capabilities, and costs.
2. Should people be allowed to use the Internet anonymously? Should ISPs be required to pay for hardware and software that can track individual usage in case of a lawsuit or criminal charge? Is it possible to prevent anonymous use of the Internet?
3. Do you think governmental agencies should share data about citizens? For example, should the FBI be able to access IRS records to locate suspected criminals? Should the FBI be allowed to access files from state and local governments? For instance, should all arrest records be automatically relayed to a central database? Should medical records be accessible to law enforcement agencies? Say that it is technically possible for the FBI to build a national database that contains DNA records for all citizens. If all medical records (from accidents, blood tests, and medical treatment) were computerized and automatically forwarded to the FBI, the agents could easily locate virtually any criminal.
4. Some remaining Federal laws limit the ability to create huge, integrated collections of personal data. Some agencies, including the FBI, have turned to buying this data from private companies (e.g., ChoicePoint). Should government agencies be allowed to circumvent laws by purchasing data on individuals from private agencies?
-  5. Research the issues involved in electronic voting. What problems need to be overcome? What technologies could be useful? Does an electronic voting system have to be perfect, or simply better than the existing manual system?
6. Should vendors be allowed to charge different prices for online products, or should everyone pay the same price? Answer the question both from the perspective of the consumer and as a vendor or artist.

7. Should consumers be able to sue software companies for security failures or other problems with the software? What limits these lawsuits now?
8. What aspects of education would you prefer to have online or automated? What elements would you prefer to keep in person?
9. Find at least five news sites on the Web. Evaluate them in terms of (1) style/presentation, (2) accuracy, (3) believability, and (4) balanced news.
10. Identify which privacy and computer crime laws might apply to the following situations:
 - a. Someone intentionally downloads a program from a Web site which is then used to run a denial of service attack on government computers.
 - b. A hospital employee sells a celebrity's health report to a newspaper.
 - c. You download and distribute copies to your friends of a software program that captures digital video and audio streams and converts them to unprotected files.
 - d. A Chinese government agent intercepts your PayPal data and uses it to buy electronics items.
 - e. Homeland Security asks your ISP to provide copies of all of your Skype conversations.
 - f. You send marketing e-mail to customers without including your business address.
11. Should Internet gambling be legal in the United States?
12. Should all consumers be allowed to pay the same price for identical items purchased on the Web?



Technology Toolbox

13. Find at least two translation sites and test them with sample text. If you read the second language, comment on the results. Translate the text back to the original language and comment on the quality.
14. Find at least two foreign exchange sites and convert \$100 (USD) into a different currency. How much does your credit card company charge for currency exchanges?
15. Why would you not want to use “Private” or “Incognito” browsing all the time?
16. Research the current status of the “do not track” option to see if there is any progress towards it becoming a standard.
17. Even with cookies blocked and “Private” browsing, explain how your Internet activities can still be tracked.



Teamwork

18. Assume that you are selling a new release for popular music. Create a silent auction and have everyone write down the price they are willing to pay for the music. Add up the numbers to get the total revenue you would obtain. Now, look up an average price for a similar item. Assume that each person who was willing to pay at least that amount would actually buy the item, and the others would not. Count the number of items sold and multiply by the fixed average price to get revenue. Compare the two values for total revenue.
19. Have each team member select a developing nation. Research the information technology available in that country. How do people get access to the Internet? What percentage of the people have used the Internet? Combine the results and create a list of options that might be used by other nations to improve Internet access.
20. Split the team into two groups to participate in a debate. The proposition is that programmers and developers should be licensed. One group should find evidence and arguments to support the proposition, the other to defeat it. If possible, conduct an actual debate. Otherwise, outline your arguments and compare them in writing.
21. Examine the arguments against electronic voting. Divide the arguments among the team members and have each person research existing technologies and proposals. Identify the methods used to avoid or minimize the stated problem. Combine the results and write a proposal defending the use of electronic voting.
22. Interview or survey at least 30 people, not students in the class and be sure to include a range of demographics including older people. Ask them what they would think about a national ID number and how it might affect them. Ask them what they think about the potential benefits and how it would be different from the existing system.
23. Split the team into three groups and have each group choose one nation. Find at least one computer-crime or privacy law for that country. Note: It helps if at least one person in the group can read Web documents in the country's language. Combine the results and summarize which crimes are most commonly outlawed.
24. Research a couple of current patent violation cases involving IT and argue why patent laws and procedures should be changed.



Rolling Thunder Database

25. What privacy problems might exist at Rolling Thunder? What rules or procedures should be enacted to avoid problems?
26. Your boss says that with the decline in sales, it would be wise to cut costs and suggests that you could buy only a single copy of some of the office software and install it on multiple machines. What do you do?



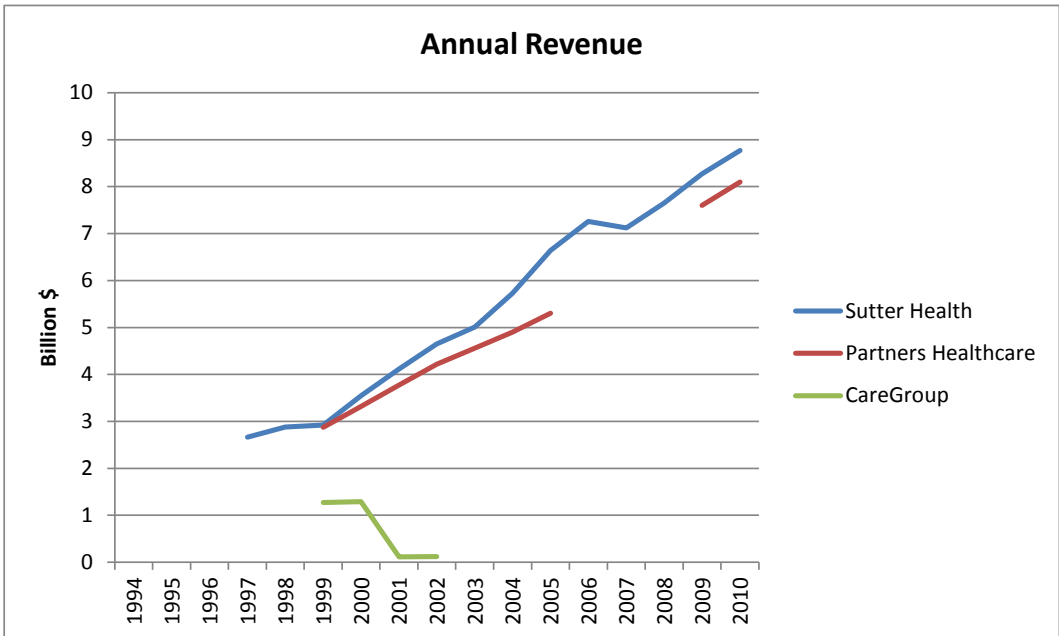
27. The management at Rolling Thunder is thinking about trying to get a patent for an online process of configuring and ordering a custom bicycle. Search the patent records to see if anyone already has a similar patent, and estimate the probability of obtaining such a patent.
28. Rolling Thunder Bicycles wants to begin sales to Europe. It is currently run completely in the United States. The company will add a Web site and establish separate contacts with bike stores in Europe. What effect will these actions have on the information system?

Additional Reading

- Arkin, William and Robert Windrem, "The U.S.-China information War", *MSNBC*, December 11, 2001. <http://www.msnbc.com/news/607031.asp>. [Description of some aspects of the U.S. information warfare preparations.]
- Collett, Stacy, "5 Legal Gotchas in the Cloud," *Computerworld* (whitepaper), April 18, 2011. [Good summary of legal issues in cloud computing in terms of where data is located and multiple contractors.] http://www.computerworld.com/s/article/355454/Legal_Risks_in_the_Cloud
- Government Computer News, January 6, 1992.
- Grosso, Andrew, "The individual in the new age," *Communications of the ACM*, July 2001 44(7), 17-20. [A readable legal perspective on individual versus society.]
- Jones, Douglas W. "Problems with voting systems and the applicable standards," May 22, 2001. <http://www.house.gov/science/full/may22/jones.htm> [Issues on electronic voting systems.]
- Kelly, Sanja and Sarah Cook, *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, Freedom House, 2011. <http://www.freedomhouse.org/uploads/fofn/2011/FOTN2011.pdf> [A summary of national restrictions and censorship on Internet traffic.]
- Machalaba, Daniel. U.S. Ports Are Losing the Battle To Keep Up With Overseas Trade, *The Wall Street Journal*, July 9, 2001. [Effect of automation on jobs at the loading docks.]
- Mercuri, Rebecca T. "Scoping Identity Theft," *Communications of the ACM*, May 2006, 49(5), p. 17. [Data and laws on identity theft.]
- Stoll, Clifford, *The Cuckoo's Egg: Tracking a Spy Through a Maze of Computer Espionage*, New York: Doubleday, 1989. [Fascinating story of a spy searching US networks.]

Cases: Health Care

The Industry



Health care makes up a substantial portion of expenditures in the United States. In 2004, health care expenditures were projected to be \$1.8 trillion, a whopping 15.3 percent of gross domestic product. As the population ages, particularly the boomers, the U.S. government estimates that these values will rise to \$3.4 trillion or 18.4 percent of GDP by 2013 (Brewin 2004). It is also a highly complex industry because the ultimate consumer, the patient, rarely bears the direct costs of the services. In 2000 (the most recent federal study), private medical insurance covered about 41 percent of total health care expenses, Medicare and Medicaid combined paid about 31 percent, and individuals paid 19 percent of the costs out of their own pockets (AHRQ 2003). The Census Bureau maintains a history of health expenditures and annually updates the projections. The 2008 actual data were \$2.3 trillion (16.2 percent of GDP), with a projection for 2015 of \$3.4 trillion. The tables also separate private and public expenditures and breakdowns for hospitalization, physician, drug, and nursing home costs (http://www.census.gov/compendia/statab/cats/health_nutrition/health_expenditures.html, Table 130). In 2008, about 53 percent of the costs were paid by private funds, 35 percent federal, and 12 percent state. Almost 12 percent of the costs were paid out of pocket by individuals, versus private insurance.

Federal Involvement in Care

Some people have heard about mistakes made in operating rooms—where the surgeon operated on the wrong knee or arm. Some patients have taken to writing on their limbs before surgery—just to make sure everyone knows which leg or arm to work on. Not as many people are aware of the problems that arise with drugs.

Physicians sometimes prescribe the wrong drug. Nurses occasionally deliver the wrong drug or incorrect dose to a patient. The federal government has stepped in to reduce this problem. The Food and Drug Administration (FDA) in 2003 issued a ruling to take effect in 2004 for new drugs and 2006 for existing drugs. All individual doses of drugs will be required to have bar codes. Hospitals will then have to implement bedside bar code readers that match patients and drugs before giving the drugs. Any errors will be flagged by the system. Hospitals are spending millions of dollars to add the new systems. In terms of those surgeries, new rulings require hospitals and physicians to adopt a marking system and mark every operating site on the body while the patient is conscious, to reduce mistakes. Apparently, they could not figure out a way to bar code the body parts.

In 2004, President George Bush stated that he wanted the entire health care system to move to electronic records. Within 10 years, hospitals are supposed to have a system that allows electronic sharing of medical data (Brewin 2004). This push goes far beyond individual hospitals. It means that the entire health care and health informatics industry has to agree on standards and has to come up with a way to identify patients and transfer data securely.

The industry has been trying for several years to devise a health care information system that would work for the entire industry. Tommy Thompson, U.S. Secretary of Health and Human Services, had asked the industry to derive a blueprint for an electronic health-record system. In late 2003, the initial plan was rejected by the industry because it was overly complex. The original design was cumbersome, yet still did not address all of the potential issues. Part of the problem is that it tried to focus on a detailed level and include everything from medical records to billing to patient history. A bigger problem is that several proprietary systems already exist, and vendors are concerned that a government-designated system would be incompatible. At this point, there is not even a framework or structure for defining the overall approach (Landro, 2003).

The federal government has also taken an interest in improving health care by reducing errors through bad information. Panni Kanyuk, a senior Datamonitor health-care analyst noted that “information technology is an important tool in improving patient quality of care, and we’re seeing this resonate in the market.” Most health-care providers surveyed responded that they anticipated increasing IT spending by at least 10 percent per year (McGee 2004).

Several medical care providers have adopted electronic systems for recording physician drug orders. The systems have the ability to reduce errors and improve communication. However, they still require physicians, pharmacists, and patients to be conscientious and observant. A study at one hospital identify 22 ways that medication errors were facilitated by a computerized physician order entry system. Although handwriting errors are no longer an issue, other problems can arise with information errors and usability problems. Ross Koppel of the Center for Clinical Epidemiology and Biostatistics at the University Pennsylvania School of Medicine observed “the largest problem is that the system asks house staff to twist the software like a pretzel rather than the software corresponding to the way the work is done” (McGee 2005).

Information technology has the potential to manage data and reduce costs and time, but the medical world is highly fragmented. Many physicians work in their own offices, and hospitals are often independent or connected into loose networks. Throw in a few dozen insurance companies, and various state and federal organizations, and even simple communication becomes challenging. A study by a re-

searcher at Sutter Health in California found that even with HER systems, physician costs are high because of the problems dealing with multiple health plans. Annual costs for even a small clinical practice were estimated to be \$51,221 for non-clinical personnel time and \$34,052 for physician time—for each physician in the clinic. The total costs of \$85,273 represented 10 percent of total revenue for a practice (Hardy 2009).

Privacy

Privacy has become a more important issue. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has finally been given some teeth. Any organization that handles medical data has to comply with rules that prevent them from releasing medical data. The rules cover accidental releases, such as overheard conversations, and security breaches.

Actually, President Bush watered down the original medical privacy rules created by President Bill Clinton. The original rules required mandatory patient consent to disclose data, even for treatment and payment. The new rules simply require that patients be notified of the privacy policies (CNN Online 2002). The main argument was that getting patient signatures might slow down the treatment process. Although privacy advocates were upset, the real-world effect was probably minimal. Most health care providers were simply requiring patients to sign a form that waives most privacy anyway.

The law has been useful at encouraging health care providers to tighten up the access to medical records. For example, hospitals cannot release or use patient data for charity solicitations. The billing system has to be separate from the medical system, so that a billing clerk could see that a patient was billed for a test but not see the test results (Tarkan 2003).

In 2010, the U.S. Congress passed a healthcare law that was not exactly popular—it was challenged in court on several grounds, and will probably eventually end up before the U.S. Supreme Court, or be overwritten when Obama leaves office. The law is known as the Patient Protection and Affordable Care Act. One of its main, and controversial, elements is that it requires everyone to buy health insurance. One of the problems often cited by reform proponents is that uninsured people cost the system billions of dollars a year because hospitals and doctors are ethically required to treat sick and injured people even if they have no insurance. And people with no insurance tend to avoid paying for routine care and wait until they have to go to the emergency rooms. The goal of the law was to help reduce the projected federal deficit due to rising Medicare and Medicaid costs (Moore 2011). Although, it is difficult to see how costs can be reduced without deliberate increases in supply.

Additional Reading

AHRQ, *Statistical Brief #27: National Health Care Expenses in the U.S.*

Community Population, 2000. November 2003. Agency for Health care Research and Quality, Rockville, MD. <http://www.meps.ahrq.gov/papers/st27/stat27.htm>

Brewin, Bob, “Health Care IT Plans Get a Renewed Push,” *Computerworld*, May 3, 2004.

CNN Online, “Change in the Air for Medical Privacy Rules,” April 16, 2002.

- Hardy, Kyle, "Study Shows Physicians Using IT Still Experience High Cost in Billing and Insurance," *Healthcare IT News*, May 14, 2009.
- Landro, Laura, "Plans for Health-Record System Need Work, Industry Players Say," *The Wall Street Journal*, September 15, 2003.
- McGee, Marianne Kolbasuk, "Health-Care Providers Pump More Dollars into I.T." *Information Week*, June 7, 2004.
- McGee, Marianne Kolbasuk, "Computerized Systems Can Cause New Medical Mistakes," *Information Week*, March 9, 2005.
- Moore, Stephen, "ObamaCare Doesn't Add Up," *The Wall Street Journal*, June 29, 2011.
- Tarkan, Laurie, "A Privacy Law's Unintended Results," *The New York Times*, June 3, 2003.

Case: Sutter Health

Sutter Health is one of the largest health care systems in northern California. In 2002, the not-for-profit organization had almost 40,000 employees and patient services revenues of almost \$4 billion. Its 26-member hospitals with 5,773 beds recorded almost 240,000 discharges in 2002 and over 2.5 million outpatient visits (www.sutterhealth.com). Like any hospital group, Sutter works to improve the health of its community. And it struggles to balance costs, medical technologies, and information technology.

Quality Care

Sutter is working to build the new systems to implement the FDA drug bar code rules and improve the quality of drug prescriptions. It is deploying 6,000 PCs on mobile carts. They will be connected by Wi-Fi wireless networks because it would be too expensive to install wires in every hospital (Cuneo 2004). One advantage to the new system is that drug manufacturers will be required to put bar codes on individual doses. They have used them on bulk shipments in the past, but that still required hospitals to repackage and remark all of the drugs. John Hummel, CIO of Sutter Health, observed that those codes will save the company about \$2 million a year (Brewin 2004).

Sutter recognized that a key part of the bar code point-of-care (BPOC) technology is that it had to be combined with a computerized physician order entry (CPOE) system. When the nurse scans patient and drug codes, the system has to verify the original drug order. That means the physicians need to enter the drug orders electronically. Sutter chose to implement a high-end BPOC system that also checks for patient allergies and asks nurses to double-check drugs if they have similar names or similar appearance to other drugs. Hummel involved nurses early in the selection process to ensure the system would be easy to use and that they would willingly adopt it. After implementation, nurses indicated a 42 percent improvement in satisfaction and a 64 percent improvement in perception of system efficiency (Johnson et al. 2004). Furthermore, the real-time dispensing data feeds directly into the charging system, so patient bills are more accurate.

One of the early challenges that Hummel faced was the need to integrate data from multiple medical systems. In 1999, he installed an interface engine from

Century Analysis, now a division of Sybase. It serves as a hub and transfers data across systems. For example, the data from the Siemens Medical Health Services that handles picture archives can be transferred to or accessed from the Lawson ERP system. In 2003, he upgraded the engine to an eGate integration platform from SeeBeyond Technology Corporation. The new system utilizes XML to transfer data quickly between even more systems. His ultimate goal is to provide a single view of all patient data. The company is using Identity Hub software, an artificial-intelligence tool from Initiate Systems, that uses statistical techniques to match historical data. It is critical that physicians accurately identify patients to retrieve the proper records. Hummel observes that “if I go to the doctor, he needs to know the difference between John Hummel and John C. Hummel” (McGee September 2003).

As of 2004, more than 1,000 Sutter physicians store patient data electronically, and more than 400 of them have totally paperless offices. Even X-rays and prescriptions are stored digitally. The goal is to have data for all 4.5 million Sutter patients integrated in 2006. The system will make it easier for patients and physicians to use the health services—regardless of location.

Hummel’s group is also building a virtual intensive care unit (ICU), where each hospital will have telecommunication links with real-time videoconferencing to an ICU physician. The ICU staff will be able to remotely monitor patients and collaborate with on-site staff. With the eICU system, one ICU physician and nurse monitor dozens of patients at hospitals that cannot afford full-time intensive care units. Keeping a physician online full-time provides additional supervision. Nurses do not have to worry about finding a doctor or surgeon for unnecessary cases. Dr. Daniel Ikeda, director of the system, notes that “when I’m in the eICU, I’m a lifeguard. I use the technology to look for troubling trends, before they become serious complications. A critically ill patient can turn sour in a matter of minutes. (Kolbasuk 2003).

The electronic ICU has been successful, based on its ability to prevent deaths and on the increasing usage found by physicians. The system was created for about \$25 million, but by 2006 had already saved 425 sepsis-related patient deaths, and cases of ventilator-associated pneumonia fell from 37 in 2005 to 8 in 2006 (Hoffman 2007)

Sutter Health is also rolling out Internet services to physicians and patients. By 2005, all Sutter physicians should have Web access, where they can download charts, check lab results, or order prescriptions. On the patient side, customers can use the Internet to communicate with doctors, view their records, order refills, or get additional instructions. The system is being used by 15,000 patients in Palo Alto (Cuneo 2004).

Sutter Health is using more sophisticated decision support and data analysis tools to help reduce errors and problems throughout the health care process. For example, a data warehouse tracks injuries that occur during childbirth, as well as the frequency of induced labor. The system is being used to reduce the instances of maternal tissue tears (McGee October 2003).

The California Pacific Medical Center in San Francisco is an affiliate of Sutter Health. The Center uses an automated Site of Care (SOC) system to enter data electronically at the bedside. The system saves time and money by reducing transcription costs. It also makes it easy to conduct studies and analyze the data. Reports can be generated quickly in response to physician queries. After a decade of

use, the system contains substantial information and knowledge that can be used to improve patient care (Parker 2002).

Pushed in part by the federal government to improve medical care by reducing errors, Sutter Health is adding more support for electronic records keeping. Hummel noted that “my IT employees aren’t making widgets, they’re saving people’s lives,” by giving physicians electronic access to information and medical records (McGee 2004). Hummel also reported that California providers were likely to implement complete electronic records in 4-5 years, ahead of the 2014 timetable set by President Bush. Perhaps fueled by the importance of the technology and the enthusiasm of Mr. Hummel, Sutter Health was ranked 18 in *Computerworld’s* 2007 “100 Best Places to Work in IT” survey.

Simply storing health records electronically does not solve all problems. Hospitals and physicians also need interoperable electronic health care records. Parsing the jargon, a key strength of electronic records is the ability to share the data with other providers. The U.S. Department of Health and Human Services is working to define standards to support interoperability within the federal government. The agency will provide some software to small and midsize physician practices at low cost (Havenstein 2005b). Sutter Health is building a system to connect its 26 hospitals and more than 5,000 physicians. CIO Hummel observed that much of the data is stored in systems purchased from Epic Systems Corp, but that Sutter’s “interface department builds over 800 interfaces a year to integrate all our vendors” (Gilhooly 2005).

In 2010, Sutter Health partnered with iTriage to offer a smartphone app that provides basic medical information including lists of 300 symptoms, 1,000 diseases, and 350 medical procedures. The system also taps a database of every doctor, hospital, urgent care clinic, and pharmacy in the nation—along with directions to health care providers in any community (Merrill 2010).

In 2011, Sutter Health began offering its electronic health record (EHR) system (Sutter Community Connect) to regional physicians in independent practices. Tying more physicians into their system makes it easier to integrate patient data. Jeff Burnich, MD and senior vice president of the Sutter Medical Network noted “To truly reinvent care, we see an imperative to connect as many physicians across our network as possible by extending an HER option to community doctors in independent practice” (Healthcare IT News 2011). The system already connects more than 12,000 caregivers and almost 450,000 patients use Sutter’s online services.

Managing the Technology

John Hummel’s IT department consists of almost 1,000 employees, with a budget of 3.9 percent of the hospital’s net revenue, spending \$105 million for operations (Cuneo November 2003). He still manages to send birthday and anniversary cards to each employee every year. But the department is busy, scheduling 750 large-scale projects for 2004 alone (Cuneo December 2003). The state of California essentially mandated the huge number of projects. In 1994, the state passed a law requiring all hospitals to be earthquake proof by 2008. Sutter Health has planned \$5 billion in capital improvements. One of the big tasks for Hummel is building a new data center to consolidate all of the servers into one secure, safe location. By 2004, Sutter had completely replaced five hospitals and is planning to rebuild six more. Building the hospitals from scratch means that information systems can be built into them from the beginning (Brewin and Thibodeau 2004).

The hospital company operates in more than 100 communities and needs a network to connect all of the facilities. In 2003, the network team installed high-speed fiber-optic links to the new data center. The 50-micron multimode fiber cable can carry 10 gigabits per second. Chris Kennedy, network engineer for Sutter Health, notes that “we didn’t want to impede our LAN system and therefore chose 10 Gbps multimode fiber. Most of our applications at the desk are pushing 100 Mbps though. With the new fiber backbone, we will be ready to easily push one gigabit from our desks without compromising our network.” Category 6 cable was run to desktops in anticipation of the need to handle gigabit speeds (Oliver 2003).

Sutter Health is also spending money to improve privacy and protect data—partly driven by the HIPAA regulations. In addition to the common security and privacy controls, the IT department has a team of a half-dozen “white-hat hackers” to continually test the system to look for problems before real hackers can find them (McGee September 2003).

Like several other hospitals, Sutter has turned to wireless networks to provide data services to physicians and nurses as they move throughout the hospital. Today, most patients are given bar-code bracelets. Nurses use a portable scanner to identify the patient, retrieve drug medication information and have the computer match the records to ensure the right patient is given the correct drug at the proper time. Sutter uses Citrix remote terminal software to improve security. Physicians and nurses basically download a screenshot that provides data, but is not stored locally, so the medical provider sees only a small snapshot of the data, not the entire patient record. The wireless network is also secured against eavesdroppers (Havenstein 2005a).

Costs

In 2002, Sutter Health raised its prices to Health Net insurance by 25 percent. After a public battle fought in newspaper ads, 20,000 Health Net members jumped to other insurers to avoid the battle. Ultimately, the two companies negotiated 15 percent annual increases.

In 2003, Sutter Health encountered a more serious public relations problem. Driven by ever-rising prices for health care, several large employers began examining prices at many of the large health care providers in California. Moreover, federal regulators have been examining overpricing claims against many hospitals. In 2003, the Service Employees International Union brought significant pricing data to the attention of several organizations, including CalPers, the large retirement investment agency. They found that five of the Sutter Health hospitals had inpatient charges that were up to 53 percent higher than the national average. Five of its hospitals were also being investigated by the federal Centers for Medicare and Medicaid Services for possible overbilling. In addition, nine of the Sutter Health hospitals had total profit margins exceeding 10 percent in 2001, compared to a state average of 3.5 percent on not-for-profit hospitals (Benko 2003). In early 2004, CalPers dropped 13 of the Sutter Health hospitals from its insurance coverage. It dropped 25 hospitals from other firms. A spokesman said “We wanted to send a message to these providers that their costs are over the top.” CalPers provides coverage for 1.2 million state employees, retirees, and their families (Wojcik 2004).

In early 2009, Sutter cut 121 jobs from its IT department in Rancho Cordova to reduce costs. The cut represents about 7 percent of its IT workforce. By that time Sutter had rolled out its electronic health records system to five of its eight

physician organizations and one hospital. The company put rollouts on hold to additional hospitals (Monegain 2009). In 2011, Sutter Health signed a contract with outsourcer Affiliated Computer Services (ACS) to run the MIDAS+ health care analytic tools. The DataVision system pulls from existing clinical data and provides reports and analyses, including comparisons with similar activities from healthcare organizations across the nation. Krystin Dozier, Vice President of Clinical Effectiveness at Sutter Health noted that “MIDAS+ DataVision provides us with the comprehensive solution we need to easily view performance across our enterprise. We are particularly excited about ‘SmartReport’ which shows us, in a volume relative, DRG-weighted priority, those clinical areas and quality issues where we can track issues and target improvement efforts” (MIDAS+ 2011).

Questions

1. What obstacles will Sutter Health face to implement a completely digital health care information system by the end of 2006?
2. Why is Sutter using a data gateway to transfer information across machines instead of standardizing the underlying systems?
3. If Sutter is so advanced in its use of technology, why are its hospitals so expensive?

Additional Reading

- Benko, Laura B., “Price Check,” *Modern Health care*, April 21, 2003, Vol 33 (16), pp. 6-8.
- Brewin, Bob, “Sidebar: FDA Mandate Could Have \$7B IT Price Tag,” *Computerworld*, March 1, 2004.
- Brewin, Bob and Patrick Thibodeau, “Earthquake Law Pushes Hospitals To Spend Big On IT,” *Computerworld*, February 16, 2004.
- Cuneo, Eileen Colkin, “Uptick In Care,” *Information Week*, November 3, 2003.
- Cuneo, Eileen Colkin, “A Project for Every Problem,” *Information Week*, December 22, 2003.
- Cuneo, Eileen Colkin, “Mobile Care,” *Information Week*, March 1, 2004.
- Gilhooly, Kym, “Rx for Better Health Care,” *Computerworld*, January 31, 2005.
- Havenstein, Heather, “Wireless Leaders & Laggards: Health Care,” *Computerworld*, May 16, 2005.
- Havenstein, Heather, “Medical Software from Feds Could Benefit Big Health Care,” *Computerworld*, August 8, 2005.
- Healthcare IT News*, “Sutter Health to Spend \$50M to Help Docs with EHRs,” April 5, 2011.
- Hoffman, Thomas, “Saving Lives Via Video At Sutter Health’s eICU,” *Computerworld*, June 25, 2007.
- Johnson, Van R., John Hummel, Terance Kinninger, and Russell F. Lewis, “Immediate Steps Toward Patient Safety,” *Health care Financial Management*, February 2004, vol 58(2).

- McGee, Marianne Kolbasuk, "Mission Critical," *Information Week*, May 19, 2003.
- McGee, Marianne Kolbasuk, "Health Care & Medical: Tech Innovation Keeps The Doctor In," *Information Week*, September 22, 2003.
- McGee, Marianne Kolbasuk, "Putting a Clamp On Medical Mishaps," *Information Week*, October 13, 2003.
- McGee, Marianne Kolbasuk, "Health Care & Medical: E-Health Revives Health-Care IT," *Information Week*, September 20, 2004.
- Merrill, Molly, "Sutter Health Uses Smart App to Boost Access to Care," *Healthcare IT News*, August 31, 2010.
- MIDAS+ Press Release, "ACS Awarded Contracts With Sutter Health and Memorial Hermann Healthcare System," April 7, 2011.
- Monegain, Bernie, "Sutter Health Cuts 121 IT Jobs," *Healthcare IT News*, May 19, 2009.
- Oliver, Carol Everett, "A Cure for Bandwidth Bottlenecks," *Communications News*, September 2003, vol 40(9), p. 26.
- Parker, Anne, "Tracking a Decade of CIS," *Health Management Technology*, April 2002, Vol 23(4), pp. 28-30.
- Weber, Joseph and John Cady, "The New Power Play in Health Care," *Business Week*, January 28, 2002.
- Wojcik, Joanne, "Citing High Costs, Calpers Removes 38 Hospitals From Blue Shield Network," *Business Insurance*, May 24, 2004, vol 38 (21), p. 4.
- www.sutterhealth.com

Case: Beth Israel Deaconess Medical Center

Beth Israel Deaconess Medical Center (BIDMC) in Boston is a teaching affiliate of Harvard Medical School. It is a not-for-profit hospital that is part of the Care-Group Health System. The hospital has 534 beds and a Level 1 Trauma Center. It is a major biomedical research university (bidmc.harvard.edu). Like all hospitals, BIDMC has worked to install information technology to help patients, physicians, and nurses.

Information Technology

Emergency rooms in a major city are always hectic. The ER at BIDMC treats 60,000 patients a year (an average of 164 per day). Triage is the standard medical practice of identifying the most severe cases and treating those first (if the treatment can reasonably be expected to succeed). But with new patients arriving constantly, and nurses and physicians rotating among cases, it can be hard to keep track of the current situation. In the old days, hospitals used white boards to list major issues—but that sacrifices patient privacy and can lead to errors if the board is not updated or erased. At BIDMC, three doctors devised a new solution: an "electronic dashboard" that consists of a four-foot wireless plasma display. Patients are color-coded for severity (red for serious) and by gender (pink

or blue). The entire ER was rebuilt with wireless technology in 2002. When a patient arrives, clerks enter registration data into a laptop, and the pertinent data is transferred to the plasma display identifying them by their initials. Unlike other hospitals, patients are immediately moved to beds. The wireless system enables clerks to come to the patients. Dr. John Halamka, CIO of CareGroup notes that “if you think of a traditional emergency department, you walk in and immediately you’re sitting at a triage desk. Maybe you’re in pain, maybe you can’t make it to the desk. Well, that’s nuts. We put you in a bed, and then the registration people come to you and take your information” (Ewalt 2001).

Physicians treating patients enter orders and diagnoses into wireless laptops, with notations transferred to the display. When a procedure is completed, such as X-rays, the corresponding display element (XR) turns green. The physician’s laptops also connect to the hospital’s primary information system, so they can retrieve medical histories. In addition to improving care, the system has made the ER team more efficient. Nearby facilities averaged 450 hours in a six-month period where they had to turn patients away. BIDMC was overloaded only 40 hours in the same time period (MSNBC 2003).

The hospital has created wireless access in some other parts of the hospital. In some wards, patients are even given laptops so that they can check their e-mail or surf the Web. Halamka observes that “unless I’m in critical condition, I need to access the outside world. People are there for a long time, so we give them PCs.” To improve privacy and security, the hospital encrypts all wireless transmissions and requires that all wireless devices be registered before being granted access to the network (Ewalt 2001).

In terms of basic data and operations, BIDMC was an early adopter of computerized drug cabinets to monitor inventory levels throughout the hospital. The cabinets have a built-in PC board running a Sybase database and a flat panel display. Located throughout the hospital, they are tied to the central pharmacy to signal when an item needs to be refilled and to provide data for patient billing (Whiting 1999). With the new federal drug bar code regulations, the drug cabinet capabilities will probably not be needed.

Patient Care

As the U.S. population gets more comfortable with online interactions, it is only natural that patients want to be able to e-mail their physicians and obtain advice or renew prescriptions. Many physicians have resisted this technology. Some have claimed they are worried about privacy and liability issues. A few more cynical observers have noted that physicians do not usually get paid for these communications. Either way, few physicians embrace online interactions with patients. In 2004, Blue Cross Blue Shield of Massachusetts began a pilot study with several health care organizations, including 200 physicians at BIDMC. Blue Cross pays doctors \$19 for each Web visit, and patients kick in a \$5 co-payment. BIDMC anticipates participation by about 250 patients with perhaps two e-visits each for the first year. Contacts and billing are handled through a secure site by RelayHealth (McGee 2004).

Within the hospital, BIDMC is moving to electronic records. It is using a Web-based order-entry system for prescriptions, lab tests, and supplies. The system includes reminders for physicians and nurses and can electronically notify them when lab results come back. Massachusetts requires that all medical data be stored for 30 years, including images such as MRI, ultrasound, and X-ray scans. In ad-

dition to meeting state requirements, the system database can be used for data mining (McGee September 2003). Physicians can access stored images almost instantly through the network. Ronald Mitchell, CareGroup's director of radiation information systems, notes that "in the operating rooms, we're installing dual high-resolution flat-panel monitors so that surgeons can view the images prior to and during procedures" (McGee October 2003).

Network Disaster

One of the challenges to an electronic medical system is that it has to keep running—24 hours a day with no interruptions. In November 2002, the network at Beth Israel Deaconess crashed and had to be completely rebuilt in a matter of days. In the meantime, physicians and staff had to resort to paper records that had not been used for years. Dr. Halamka, the CIO, widely reported the problems he encountered, to show other hospitals how to improve their networks.

On Wednesday, November 13, 2002, Halamka noticed that the network was sluggish and taking too long to send and receive e-mail. He talked with the network team, and they had already noticed the problem. It appeared to be coming from a surge in one of the switches. They had experienced these spikes before, but happened to have a consultant on-site looking into the problem with that switch. To help identify the problem, network engineers began shutting down virtual LAN (VLAN) segments. That action was a mistake, because it forced the switches to recalculate the traffic distributions, and all data traffic ground to a halt while the switches continually reconfigured. They quickly turned everything back on, but the network was still sluggish. Around 9 P.M., the engineers spotted the problem: a loop in the spanning tree protocol. When data arrives at a switch, the switch computes the shortest path and directs the message to the destination. The problem was that the spanning tree could only look out to seven hops. Once data travels beyond seven jumps, it can lose its way and get redirected to the beginning—creating a loop. On Wednesday, a researcher had loaded several gigabytes of data into a file-sharing application, and it looped, clogging the network. The network team took standard steps to cut links and reduce the probability of loops and went home for the night.

The next morning, as usage ramped up, the network slowed to a crawl again. The team tried other options with no success. The network was beginning to cause problems for the physicians and patients. One physician was monitoring a critical patient and needed several lab reports to help spot the problem. But it was taking five hours to get lab reports completed. Fortunately, the patient survived. At 3:50 P.M., the hospital closed its emergency room for four hours.

At 4:00 P.M., Halamka called Cisco, their network provider. Cisco triggered its Customer Assurance Program (CAP) where the company commits every resource possible to solving the problem. A nearby team from Chelmsford moved in and set up a command center. Their first problem was that the network was so slow they could not get status information from the switches. They finally found some ancient 28.8Kbps modems to use to bypass the network and found the problem at 9 P.M.. The image archive system was 10 hops away from the closest core network switch. Huge volumes of data were being abandoned because the spanning tree system could only go out to seven hops. The problem was that the network had been cobbled together since 1996 one piece at a time, using outdated switching technology. The team decided to upgrade the backbone to the image system with a Cisco 6509 router/switch. The router element provides more sophisticated com-

munications by constantly evaluating bandwidth and rerouting traffic as needed. Shortly after 9 P.M., Cisco loaded a 6509 onto a commercial flight from San Jose to Boston. Working through the night, the CAP team rebuilt the image network, a task that originally took six months.

The next morning, when the load increased again, the network still began to crash. By 10:00 A.M., Halamka decided to shut down the entire network and revert to paper. Most of the medical staff had already given up on the system anyway. Employees cranked up the copiers to generate blank forms. Some interns and physicians had never used paper prescription forms before and had to be trained. Runners were used to carry the paper and communicate orders.

By Saturday morning, the system was still down. The engineers decided the entire network was outdated. At 5 A.M., three additional Cisco engineers arrived from Raleigh. At 8 A.M., two more 6509 routers arrived by plane from Cisco. The team of 100 people spent the day building a new network. By Saturday night, the new core network was in place. But it took most of the night and Sunday to debug small glitches, such as a dead network card and out-of-date firmware. On Monday morning, the network was finally stable. At noon, Halamka declared the crisis over (Berinato 2003).

The main lesson from the disaster: networks have to be evaluated on a continual basis. You cannot just plug new items in and expect everything to work correctly. You need to have an overall architecture that supports the entire system. And you have to be willing to rebuild and replace core equipment as new technologies are introduced.

Moving Forward

After rebuilding the network and SQL Server databases with highly-redundant systems, the IT system has succeed since 2004 with better than 99.9 percent uptime (Halamka 2007). With the main network problems solved, Beth Israel Deaconess Medical Center continued to expand its use of information technology. In 2004, the hospital, along with the parent company CareGroup, Inc., began installing RFID tags that can be read by hardware from PanGo Networks, Inc. that ties into the wireless Wi-Fi network at the hospital. The hospital is using the tags to track equipment—the PanGo software provides a map of the location of expensive equipment. Halamka noted that the two-campus hospital has millions of dollars of expensive equipment and loses almost \$400,000 of equipment a year, “because in the course of normal care, it gets misplaced” (Rosencrance 2004). The system can also be used to monitor the location of medical workers to help locate them in an emergency, or even to locate patients in the future.

Beth Israel Deaconess is one of 31 hospitals in 10 large cities tapped by the Centers for Disease Control and Prevention to provide automated data feeds from its emergency rooms. The CDC is concerned about pandemics and terrorist threats and uses the real-time data collection to help spot early trends. Barry Rhodes, associate director for technology and informatics in the Division of Emergency Preparedness and Response at the CDC observed that “the amount and rate of data streams to CDC is really unprecedented [compared with] what we have done in the past” (Havenstein 2006).

Beth Israel Deaconess and a few other medical providers have begun making patient data available directly to patients via Web sites. Although many are wary of potential privacy issues, the practice has the ability to keep patients more involved, and it gives them the ability to spot and correct errors in the database (McGee 2007).

Beth Israel was one of the first big hospitals to adopt the Apple iPad as a useful device for interacting with physicians. CIO John Halamka was even featured in an Apple video. He noted that “Sometimes doctors are overwhelmed with data. What we have tried to do on the iPad is give doctors at the point of care the tools they need at the exact moment the doctor can make a difference.” The doctors can use the devices to retrieve data and even show images to the patients (Merrill 2011).

Questions

1. How does the emergency room system at BIDMC protect patient privacy?
2. Why have physicians been so slow to adopt online and e-mail communications from patients?
3. Why did the BIDMC network get so bad and fail? Why was it not fixed earlier?

Additional Reading

Berinato, Scott, “All Systems Down,” *CIO*, February 25, 2003.

Ewalt, David M., “CareGroup’s Wireless Hospital,” *Information Week*, September 17, 2001.

Halamka, John, “Conservation of Aggravation,” *Computerworld*, January 15, 2007.

Havenstein, Heather, “CDC Upgrading IT to Gather Data From Hundreds of Hospitals,” *Computerworld*, February 13, 2006.

McGee, Marianne Kolbasuk, “Health Care & Medical: Tech Innovation Keeps The Doctor In,” *Information Week*, September 22, 2003.

McGee, Marianne Kolbasuk, “Putting A Clamp On Medical Mishaps,” *Information Week*, October 13, 2003.

McGee, Marianne Kolbasuk, “E-Visits Begin To Pay Off For Physicians,” *Information Week*, May 31, 2004.

McGee, Marianne Kolbasuk, “Doctors Debate Giving Patients’ Online Access To Health Data,” *Information Week*, May 26, 2007.

Merrill, Molly, “iPad 2 Looks Even Better for Doctors,” *Healthcare IT News*, April 8, 2011.

MSNBC, “Next Frontiers: Using Technology To Get Ahead In Business,” February 3, 2003.

Rosencrance, Linda, “Boston Hospital Will Track Assets with Wireless System,” *Computerworld*, September 20, 2004.

Whiting, Rick and Bruce Caldwell, “Data Capture Grows Wider,” *Information Week*, June 14, 1999.

Case: Partners Health care System

Partners Health care System, Inc. is an association of hospitals in the Boston area, including Brigham and Women's Hospital and Massachusetts General Hospital. The not-for-profit organization had revenues of \$4.6 billion in 2003. Across the organization, the physicians and staff see 11,000 patients a day (annual report on the company Web site www.partners.org).

Telemedicine

With support from engineers at MIT, the hospitals in Partners were pioneers in the use of telemedicine. The system was created to expand the reach of the organization and provide quality care to patients in outlying areas. The system originally ran on ISDN phone lines with videoconferencing equipment. In 2000, the organization turned to an Internet-based system using Microsoft Windows 2000 Advanced Server. Dr. Joseph Kvedar, director of the Telemedicine Program, notes that “with the help of Windows 2000 Advanced Server, we will be able to extend the reach of our providers around the globe and to take the considerable body of knowledge within our organization and make it available virtually anytime, anywhere” (Microsoft 2000). The system is integrated into Microsoft's Internet Information Server (IIS) to exchange data and information as well as provide video streaming. The unit estimates that there are 20,000 potential users in one target group alone, and the system might eventually reach hundreds of thousands of users. Scalability and network load balancing were critical factors in upgrading the system. To access the system, users need only a Web browser and an Internet connection, as opposed to proprietary commercial lines that were needed with the old system (Microsoft 2000).

Telemedicine offers the possibility of providing detailed expert services to many new areas. However, some serious obstacles remain. Notably, insurance companies are reluctant to pay for the services. In part, they are concerned about fraud and billing abuse. Despite the obstacles, Kvedar says that Partners has seen e-visits increase by 25 percent a year (Kolbasuk 2004). Some home-health nurses are turning to digital cameras and camera-equipped cell phones to treat basic skin problems. They take photos of skin wounds on diabetic patients and transfer them via the Internet to wound specialists. The specialists can examine the patterns using the digital history files. They can also check progress on many patients in one day. Partners is equipping up to 180 nurses with digital cameras or high-resolution cell phone cameras to provide care for 2,800 at-home patients (Kolbasuk 2004).

Knowledge Management

Medicine revolves around a tremendous amount of knowledge. Some of it is generated by research, some by best practices, some by experience. In the mid-1990s, medical researchers were concerned about the high error rates at Brigham and Women's and Massachusetts General hospitals. Sometimes simple things were causing huge problems—such as physicians not knowing a patient's allergies or forgetting that two drugs had bad interaction effects. So, they built a knowledge management system to assist physicians prescribing drugs. Doctors enter orders into the computer and it examines patient data, test results, other drugs, and diagnostic information to evaluate the drug choice. It then makes recommendations. John Glaser, CIO at Partners, notes that serious medication errors have been reduced by 55 percent, and “about 400 times a day, a physician changes his mind on an order based on the computer” (Melymuka 2002). Although that is only 3

percent of the total drug orders, it can save lives. Because the system provides only concrete advice that is not debatable, physician acceptance has been fairly good—even though entering the data can add 30 minutes a day to their workload. One physician even thanked Glaser: “I just want to tell you our system has saved my ass a couple of times” (Melymuka 2002).

Unfortunately, Glaser notes that “Only about 3 percent of hospitals have systems like this. That’s because it’s hard, but also because the ROI is fuzzy and messy” (Melymuka 2002). The low adoption rate is one of the reasons for the push by President Bush to force hospitals to move to electronic records and track drugs with bar codes. The Center for Information Technology Leadership backed by Partners notes that if the industry can standardize on electronic records, hospitals and insurers could save \$86 billion a year (Brewin 2004).

Technology Management

One problem with technology that is rarely discussed outside of IT departments is that individual users often want new projects or special treatment. Special requests can be important and they can be useful, but individual users usually want their pet projects to move to the top of the list. Particularly in healthcare, it is easy for some to argue that their projects can save lives. But, if the IT department spends all of its time responding to special requests, no time will remain for the big projects. Partners Healthcare experienced these problems—particularly since the department did not have a means to track all of the special requests. Mary Finlay, deputy CIO, said the team counted over a 100 ways special requests arrived and that they “were marginalizing resources by spreading them across the special requests plus the major initiatives.” To solve the problem, the IT department added a tracking system to handle evaluation and approvals of nonscheduled projects (Artunian 2005).

John Glaser, CIO of Partners Healthcare, realized a major problem was brewing in July 2004. The electronic medical record (EMR) system serving 6,000 physicians and nurses had been suffering from minor problems since the start of 2004, but in July and early August, the system appeared to be melting down—with frequent outages and slowdowns. Partners, Boston’s largest hospital group, had been using EMR for 15 years—largely adopted by two big hospitals: Massachusetts General and Brigham and Women’s hospitals. The system continued to degrade in August and the IT staff did not have solid answers for the causes. Mr. Glaser brought in IBM consultants, but also spent considerable time deflecting and absorbing criticisms from physicians. He recognized that he had to be visible and talk with the doctors, noting “they are angry and upset, and they want to yell at someone, and it has to be you. You have to roll with it. You have to resist the temptation to fight back.” Eventually, his team found the root cause of the problem: failure to upgrade an older operating system that could not handle the load. It required three months to upgrade the system and test everything, but the staff added additional servers to reduce the outages. By the end of December, the new system was in place and working well (Worthen 2005).

Within the general shortage of IT workers in 2010, the issue of hiring for hospital IT is an even greater problem. For example, hospitals located in smaller communities would have problems attracting top talent. Located in Boston, Partners does not have that problem, but Sue Schade, CIO at Brigham and Women’s Hospital, part of Partners, noted that recruiting was problematic because the hospital runs its own custom system—not one of the standard systems in the industry such

as Epic or Meditech. So, it is not possible to find people with experience, and they have to be trained specifically for the custom system (Monegain December 2010).

New Technologies

In 2005, Partners Healthcare created a pilot project to equip home health care nurses with camera-equipped cell phones. The nurses use the phones to take pictures of wounds and skin lesions and send them immediately to specialist nurses trained in enterostomal therapy (wound care). Doug McClure, corporate manager for telemedicine technology solutions, noted that “there are only so many patients these wound-care nurses would be able to see in a day—and there’s only so many of these specialty nurses available.” The technology will enable them to work on cases more efficiently. The initial cell phone cameras had limited resolution (1 megapixel), but the organization is looking for higher-resolution phones as the technology improves (McGee 2005). The hospital is also working with Ambient Devices to help remind chronically-ill patients to take their medicine. When patients open a smart pill box, an electronic message is sent to the hospital. The hospital computer then remotely turns a special light at the patient’s house from red to green (McGee 2006).

In 2010, Brigham’s was one of the hospitals in 15 communities to receive a share of \$220 million from the federal government to serve as models for widespread use of healthcare information technology. Jonathan Teich, MD, who is an assistant professor at Harvard and works as an attending physician in emergency medicine at Brigham and Women’s Hospital among other jobs noted that “We can read all about how to do it, and we can read books and guidance, but I think that providers really want to see examples of how it’s working somewhere else, someplace like them” (Monegain June 2010). The cities became known as Beacon Communities, and each selected specific and measureable goals for improvement.

In 2011, Partners was one of several hospitals to adopt IBM’s business analytic technology to examine effectiveness and potential safety issues of pharmaceuticals across a large population of users (Healthcare IT News 2011). The Netezza data warehouse tool will allow researchers to analyze data from millions of de-identified patient records. Examining the massive number of cases across time might reveal interactions or other effects that would be difficult to spot in smaller studies.

Questions

1. Why did it require a federal law for hospitals to adopt bar code systems for drug prescriptions and delivery in hospitals?
2. What are the drawbacks to telemedicine?
3. What will it take for telemedicine to be used more often?

Additional Reading

Artunian, Judy, “Over the Transom: Dealing With ‘Just-this-once, ple-e-e-ase!’ IT Project Requests,” *Computerworld*, November 28, 2005.

Brewin, Bob, “Health Care IT Plans Get a Renewed Push,” *Computerworld*, May 3, 2004.

Healthcare IT News, “Vendor Notebook: DiagnosisOne Launches New Informatics Platform,” May 6, 2011.

- Kolbasuk McGee, Marianne, "E-Health On The Horizon," *Information Week*, May 17, 2004.
- McGee, Marianne Kolbasuk, "Digital Images Unleashed," *Information Week*, July 11, 2005.
- McGee, Marianne Kolbasuk, "Dude, It's Time to Take Your Medicine," *Information Week*, October 3, 2006.
- Melymuka, Kathleen, "Knowledge Management Helps Cut Errors by Half," *Computerworld*, July 8, 2002.
- Microsoft, "Partners Health care System, Inc.," February 17, 2000.
- Monegain, Bernie, "Health IT By Example," *Healthcare IT News*, June 2, 2010.
- Monegain, Bernie, "IT Staffing Troubles Ahead for Hospitals," *Healthcare IT News*, December 1, 2010.
- Worthen, Ben, "Glaser Faces the Music," *CIO Magazine*, February 1, 2005.

Summary Industry Questions

1. What information technologies have helped this industry?
2. Did the technologies provide a competitive advantage or were they quickly adopted by rivals?
3. Which technologies could this industry use that were developed in other sectors?
4. Is the level of competition increasing or decreasing in this industry? Is it dominated by a few firms, or are they fairly balanced?
5. What problems have been created from the use of information technology and how did the firms solve the problems?