Managing Technological Challenges

Technology fosters change and more change. Technological change has raised ethical and social questions of privacy, security, ownership, health, and safety. What are the implications of this fast-paced change on our society and those who live in it? Moreover, who is responsible for determining how much technological change should occur or how fast things should change? Should technology be controlled, and if so, who should be in charge of managing technology and the challenges it poses for humans and cultures in our global community?

This chapter focuses on these key learning objectives:

- Evaluating the initiatives businesses have taken to protect the privacy of their stakeholders.
- -Assessing how secure information is in a free-access information society given the vulnerability to hackers, viruses, and computer worms.
- Understanding how businesses manage technological change.
- Analyzing threats from and safeguards taken in response to the Internet pornography industry.
- -Assessing violations of intellectual property and how business and government attempt to prevent these illegal actions.
- Recognizing the ethical and social challenges that arise from technological breakthroughs in science and medicine.

Technology raises serious ethical questions regarding our privacy and the security of information, as shown by the following examples.

> Japan is one of the safest countries in the world when it comes to violent crime, but the country experienced a nearly 50 percent rise in incidents of cybercrime in 2005. Technology-based lawbreaking included fraud, prostitution, and pornography involving minors, illegal access of Web sites, and the use of spyware (software that secretly gathers information about a person through his or her Internet connection) to steal personal data.
>
> Privacy advocates sharply criticized Internet service providers in the United Kingdom for leading the push for online data retention across Europe. This effort was designed to investigate terrorism and organized crime. Despite cries of violations of personal privacy, European firms increasingly were retaining customer information and making it available to various government agencies.[1]

Are businesses and governments winning the battle of the management of technology, particularly in regard to the challenges of maintaining the privacy and safety of those using technology? Does the significant increase in technology-based crimes justify stronger government controls and more intrusion in our

technology-laden lives? Where should the line be drawn between safeguarding personal privacy and the government's need to protect the citizenry?

Bill Joy, Sun Microsystems' chief scientist, warned of the dangers of rapid advances in technology:

> The experiences of the atomic scientists clearly show the need to take personal responsibility, the danger that things will move too fast, and the way in which a process can take on a life of its own. We can, as they did, create insurmountable problems in almost no time flat. We must do more thinking up front if we are not to be similarly surprised and shocked by the consequences of our inventions.[2]

As this quotation implies, technology poses numerous challenges for society. These include issues of privacy, security, ownership, health, and safety. This chapter addresses these issues and how, if, and by whom they should be managed.

Businesses Protecting Privacy

The presence of information technology at work today is ubiquitous. Employers can use new sophisticated technology to monitor employees' movements, computer usage, and personal and work interactions. Many of these issues are discussed in Chapter 18. In response to employees' complaints that these practices are invasions of their privacy, many businesses have developed a **privacy policy**, which explains what use of the company's technology is permissible and how the business will monitor employee activities. Columbia/HCA Healthcare, for example, issued an "electronic communication policy" to its employees warning them that it might be necessary for authorized personnel to access and monitor the contents of their computer's hard drive.

The use and dissemination of employee information has been challenged in new ways and from all sides since the 2001 terrorist attacks on the United States:

Hamburgische Electricitats-Werke, a German utility company, was ordered by the German government to turn over all of its employees' records so that they could be searched for terrorists linked to the September 11, 2001, attacks. Although management at the firm had close ties with American culture and values and sympathized with the government's efforts to aid the U.S. investigation, the company refused. The head of the company, Joachim Broers, had a favorite saying: "Liberty dies by inches." He felt that the government request was a threat to liberty and the privacy rights enjoyed by his German employees.

The debate over protection of privacy versus government access to personal data has continued to rage since 2001. In early 2006, the European Union passed legislation that required firms to retain employee records and submit this information to the government in particular situations involving national security or threats of suspected terrorism. Later that year, however, the European Union's highest court struck down this law, saying the EU had overstepped its authority by agreeing to require firms to provide the United States with personal details about airline passengers, Internet users, and other such information.[3]

Issues of privacy spill over into the business–consumer relationship. Most Americans mistakenly believe that when they see a privacy policy on their popular Web site that those sites are not collecting or selling their personal information and online activities to others. According to a Minnesota Department of Public Safety report, a company could purchase the personal data information of all Minnesota driver's license holders for $1,500; by 2006, 800 companies had done exactly that. Other consumer misconceptions or simple lack of awareness regarding privacy are shown in Figure 14.1.

Recent technological advancements have increased the number of ways that privacy violations may occur. For example, Radio Frequency Identification (RFID) technology was featured in a clever television commercial where "the packages knew the truck was lost" before the driver did. Other benefits of the use of RFID technology are becoming evident, as discussed in Chapter 13. Yet, many experts have raised ethical questions about the ways RFID technology enables businesses, governments, and criminals to gather information about presale, sales transaction, and postsales activities.[4]

The increase in the number of cell phones enabling users to take clearer pictures of what is happening around them has raised various privacy objections. Sometimes this technology has aided law enforcement in capturing criminals, who were caught breaking into an automobile or store. But in other cases, people felt that their privacy was violated when they were caught in a romantic or embarrassing situation.

Industry and Government Efforts to Manage Privacy

Businesses have made a number of efforts to manage stakeholder privacy. The Platform for Privacy Preference Project (P3P) provides users with software that enables them to define which pieces of personal information they are willing to divulge on the Internet. The software also alerts consumers when businesses request additional information and asks what these businesses plan to do with it. P3P has been added to some Internet browsers at no additional cost or is available to be downloaded

free off the Internet.[5] (Chapter 16 provides additional discussion of consumer Internet privacy issues.)

In addition to undertaking efforts to protect their own customers' privacy, some businesses have banded together with others to support industry self-regulation to combat technological abuses.

Nineteen companies, including AT&T, Cisco Systems, IBM, Hewlett-Packard, Microsoft, and Oracle, contributed a total of $750,000 to launch the Information Technology–Information Sharing and Analysis Center (IT-ISAC). IT-ISAC is run by Internet Security Systems, and other technology firms can join the alliance for $5,000 a year. Through this alliance, companies can share sensitive information about cyberattacks and vulnerabilities in their software and hardware products.[6]

Although some companies have addressed the issue of Internet privacy, some skeptics believe international government supervision of the Internet is necessary. However, such international management of technology is difficult to achieve.

U.S. and European officials took a positive step in the direction of international privacy protection in the early 2000s. U.S. companies had been seeking a way to conduct business in Europe without risking lawsuits and prosecution for violating Europeans' privacy. The European Commission agreed that personal data could be collected and used by U.S. Internet companies only under certain conditions. The subject had to give consent unambiguously, and the data had to be necessary to complete a contract (such as for billing), be required by law or to protect the company's vital interests, or be needed for law enforcement. These steps earned the EC the title of "Privacy Cop to the World" and served as a model for similar privacy regulation in Canada, Australia, New Zealand, and countries in South America and Asia.[7]

Nevertheless, it will be difficult to achieve international government control of privacy, especially as it pertains to the Internet. The management of privacy may need to come from the Internet companies themselves.[8]

The Management of Information Security

Businesses have become acutely aware of the importance of maintaining information in a secure location and guarding this valuable resource. How best to manage information security remains a major challenge for businesses.

In May 2005, Time Warner reported that a cooler-sized container of computer tapes containing personal information on 600,000 current and former employees had been lost, apparently during a trip to a storage facility. A month later, Citigroup informed its customers that computer tapes containing personal information on nearly 3.9 million customers were lost by the United Parcel Service while in transit to a credit reporting bureau. The public's fears were heightened just 12 days later when MasterCard International reported that more than 40 million credit card accounts might have been exposed to fraud through a computer security breach at its payment processing company. The announcement came after law enforcement officials and company experts had identified a pattern of fraudulent charges that were traced to an intrusion at CardSystems Solutions in Arizona, which processes more than $15 billion in payments annually for small and midsized retail businesses and financial institutions.[9]

In these incidents, human error had placed personal information at risk. Sometimes, threats to our privacy come from criminals. The number of reported computer virus infections is increasing, despite efforts to detect or prevent their intrusion. Most viruses are carried in file attachments and are activated when users click to open them. A new form of the virus, a computer worm, attacked computers through the Microsoft Windows operating system in 2003.

Winding its way through the Microsoft Windows operating system, a computer worm, known by a variety of names—W32.Blaster, MSBlast, and W32/Lovsan—infected tens of thousands of home computers and corporate networks worldwide in 2003. Although Microsoft knew for months that it would be launched and tried to warn its users that the worm would appear, many users neglected to download up-to-date virus protection or install Microsoft's protective program.

The worm spread throughout North and South America, Europe, Asia, and Africa by slipping into a computer connected to the Internet or to another machine on the same network. Unlike many other kinds of viruses, the worm required no human intervention, such as downloading an e-mail message or clicking on an e-mail attachment. Once lodged in a computer, the worm could scan a network looking for other machines with the same vulnerability and try to infect them. The infected computer became sluggish and, in some cases, crashed and automatically rebooted itself several times. The worm also instructed other computers to continue pelting the site.[10]

But a more troubling recent phenomenon regarding worms or viruses is the decreasing amount of time information technology managers have to patch their software before the worms hit. As the creators of the worms became more skilled at infiltrating computer systems, the response time has dramatically shortened. Some of the recent worms and a timeline indicating their impact on businesses are shown in Figure 14.2.

"The basic message is: The world is getting worse . . . more and more out of control," said Peter Tippett, chief technology officer at TruSecure.[11]

The corporate nemesis responsible for creating and spreading computer viruses and worms is called a computer hacker. **Computer hackers** are individuals, often with advanced technology training, who, for thrill or profit, breach a business's information security system. Businesses are not the only organizations vulnerable

to the predatory practices of hackers, as some prestigious universities found out in 2005. This incident is described in Exhibit 14.A.

Businesses' Responses to Invasions of Information Security

To address the number, severity, and ease of hacker attacks on businesses, firms began to see the necessity of investing more resources into protecting their information. Firms tried to quickly respond to this growing demand.

> PricewaterhouseCoopers launched a new subsidiary to provide storage for *digital certificates*, encrypted computer files that can serve as both identification cards and signatures online. The subsidiary, called eTrust, added a 950-person network of computer security consultants already employed at PricewaterhouseCoopers.

By 2006, aggressive company security measures seemed to have turned the tide against escalating security intrusions. As software became more secure and affordable, by 2005 two out of every three computer attacks were intercepted. While some high-profile viruses made the headlines, the overall invasions into company security systems declined. One in every 36 e-mails, or less than 3 percent, contained a virus in 2005, down from 6 percent in 2004.[12]

When a group of suspected hackers broke into a U.S.-based computer system, they thought they had successfully penetrated the security system guarding an important Web site. Rather, they had technologically walked into a *honeypot*, a system used by security professionals to lure hackers to a fabricated Web site where the hacker's every move can be tracked. Lance Spitzner, creator of numerous honeypot traps, posted his findings of hacker activities on the Internet for the security community to see and learn from these discoveries.[13] Another method some businesses have used to reduce criminal intrusion of their sites is to pay hackers for their proprietary methods—so others will not use them.

> A Russian hacker, simply known as "Bit," spotted a defect in Microsoft's Internet Explorer Web browser that made it vulnerable to attack. Bit simply had to go to Web-hack.ru, a Russian Internet storefront, to offer to sell his discovery to the highest bidder. Organized crime reportedly would pay top dollar for information that would break into corporate databases and pilfer people's identities. Typically efforts were made to detect these actions and prosecute the offenders. But in 2005 computer security firms decided on a different approach and created legitimate markets for hacker intelligence. The firms offered to purchase tips from some of the very people they were trying to arrest. Critics said that this was akin to rewarding hackers for uncovering computer loopholes but security firms retorted that this free market approach would give them critical information so they could boost their protection for their clients.[14]

The Chief Information Officer

The responsibility of managing technology with its many privacy and security issues for business organizations is entrusted to the **chief information officer (CIO)**. Many firms have elevated the role of their data processing managers by giving them the title of chief information officer. More CIOs report directly to the company's CEO (42 percent) than to the CFO (23 percent). Primarily the CIO is expected to reduce costs through efficiency and productivity, enable or drive business innovation, and create or enable a competitive advantage for the company. "It's the sharp edge of the business, a tool for revenue generation," explained William E. Kelvie, former CIO of Fannie Mae. "Every business needs an executive who can harness the latest technology to reach out to customers and suppliers with seamless, up-to-the-minute data communications."

The benefits of having an innovative CIO were clear to most businesses. Peter Solvik, CIO at Cisco Systems, was credited with slashing $1.5 billion in costs by using Internet technologies for everything from human resources to manufacturing. At General Electric, CIO Gary Reiner was responsible for moving $5 billion in goods and services through the Internet, which helped improve the company's operating margins. Dawn Lepore, CIO at Charles Schwab, discovered that online trading cost only 20 percent as much as conventional trading and helped boost the firm's gross operating margin. The job of implementing these fundamental changes in business operations increasingly was entrusted to the company's CIO, whose duties now involved much more than keeping the computers properly functioning.[15]

CIOs increasingly must see the big corporate picture. The CIO must set, align, and integrate an information technology vision with the company's overall business objectives. The CIO serves as the "coach" in guiding the information technology resources of the firm toward the long-term business goals.

Internet Pornography

Many believe that the Internet pornography industry, containing sexually explicit writing or images intended to arouse sexual desire, is the most active and lucrative area of e-commerce. As of 2006, there were 4.2 million pornography Web sites, 372 million Web pages, and 2.5 billion daily pornography e-mails worldwide. Pornography downloads accounted for 35 percent of all Internet downloads. Experts estimated the annual revenues of the pornography industry at $57 billion worldwide and $12 billion in the United States alone.[16] The popularity of adult-oriented Web sites was seen when Victoria's Secret, a maker of women's lingerie, launched a fashion show on the Internet. The company reported that 1.5 million viewers logged on to see its merchandise.

Some countries aggressively monitor and try to control activities associated with these Web sites for objectionable adult-oriented materials. Yahoo! Japan, Japan's most popular Web site, had its Tokyo offices raided by police investigating the possible sale of illegal pornographic material on its auction site. This raid followed action taken against the parent company, U.S.-based Yahoo!, Inc., which was ordered by the French government to block French users from accessing Nazi memorabilia on its U.S. servers. Later, Yahoo! removed all adult-related advertising and products, such as videos, from its Web sites.[17]

Many adult Web sites ask users to verify that they are of legal age. This control is easily circumvented. In response to parents' interest in preventing their children from accessing adult-oriented Web sites, a number of new businesses emerged. For example, several major Internet companies launched a site called GetNetWise.[18] It provides parents with information on adult-oriented Web sites, including reading material and downloadable software that could safeguard their children when they are online. Other commercial porn-blocking software includes Cyber Sitter, Cyber Patrol, Net Nanny, Cyber Sentinel, Norton Parental Controls, Cyber Snoop, and Child Safe. These programs work with the Internet browser to block out violent or X-rated Web pages.

In 1998, President Clinton signed into law the Child Online Privacy Protection Act, also mentioned in Chapter 16. The primary goal of the Act is to give parents control over what information is collected from their children online and how such information may be used. The Act specifically applies to children under 13 years of

age. In addition, the U.S. Supreme Court ruled in 2003 that Congress has the right to force public libraries to install Internet filters on their computers even though such filters often inaccurately block access to legitimate Web sites.[19]

Protecting Intellectual Property

With advances in technology, protecting the ownership of *intellectual property* has become more challenging than ever. The ideas, concepts, and other symbolic creations of the human mind are often referred to as **intellectual property**. In the United States, intellectual property is protected through a number of special laws and public policies, including copyrights, patents, and trademark laws. Not all nations have policies similar to those in the United States. With the ease of accessing information through technology, especially the Internet, have come serious questions regarding protecting intellectual property. From software and video-game piracy to downloading copyrighted music and movies for free, many new means for using others' intellectual property have unlawfully emerged.

Software Piracy

[illegible]

Companies have sought assistance on the issue of software piracy from governmental agencies and the courts both inside and outside the United States. For example, the Argentinean Supreme Court upheld a lower court ruling that the country's antiquated copyright laws did not cover software, thus denying software manufacturers any legal basis to attack those with pirated materials in Argentina. However, the outcry from U.S. software makers and vendors was so strong that within months the Argentinean Chamber of Deputies made software piracy a crime punishable by fines or imprisonment or both. In 1998, the United States passed the **Digital Millennium Copyright Act**, making it a crime to circumvent antipiracy measures built into most commercial software agreements between the manufacturers and their users.

In China, where experts estimate that 90 percent of all software in use is unlicensed, government officials took steps in 2006 to curb piracy. The Chinese government announced that computer makers must ship all their product with licensed operating systems preinstalled and inspected all government computer systems for licensed software. Some of their motivation was economic, as China was poised to develop a massive technology-based communications industry. "This is good news, marking a clear step in the right direction to reverse the serious problem of software piracy that frustrates the development in China for both foreign and domestic vendors," explained Gregory Shea, president of the Beijing-based United States Industry Technology Office, which represents more than 6,000 technology companies.[21]

Since 1988, the Business Software Alliance (BSA) has been an international representative for the world's leading software companies before governments and consumers. BSA sought to educate computer users on software copyright laws, lobby for public policy that would foster innovation and expand software companies' trade opportunities, and aggressively fight against software piracy. Its members include Apple Computer, Corel, Macromedia (Asia), Microsoft, Symantec, and many other influential organizations in the software industry.

Some firms attacked those who sold or distributed pirated software. Sega of America Inc. shut down 185 Web sites, including auctions on eBay and Amazon.com, which allegedly sold pirated game software. Citing the Digital Millennium Copyright Act of 1998, a Sega spokesperson commented,

"We're using this act to send a clear message [to the Web sites and other companies]. They are liable for the content that is on their service."[22]

Pirating Copyrighted Music

By the late 1990s, technology enabled individuals to download music from the Internet at a faster pace than ever before and to store the music for repeated listening. Individuals downloaded millions of songs onto their computers, burned them onto CDs, and had their favorite collections of songs available for their listening pleasure whenever they wanted—all without the cost of purchasing the music. This process denied legitimate compensation to the artists who created the music and to the companies that manufactured or distributed these artists' CDs.

The pirating of copyrighted music is a growing and widespread epidemic. According to the International Federation of the Phonographic Industry, 20 billion songs were illegally downloaded or swapped in 2005, or one out of every three musical disks sold in the world, with sales totaling $4.6 billion. Nine out of 10 recordings in China were pirated, and 75 percent of Singaporeans surveyed said they had no personal objection to using pirated material.[23]

In the United States, the Recording Industry Association of America (RIAA) launched a series of lawsuits aimed at prohibiting illegal copying of music, protecting the legal property of the authors or publishers, and assuring that profits earned from music sales be distributed to those holding the copyrights. These actions are profiled in the discussion case at the end of this chapter.

Trade associations in other countries also joined in the battle against illegal music downloading.

The International Federation of the Phonographic Industry (IFPI) announced in 2004 that 247 people in Denmark, Germany, Italy, and Canada were served with international lawsuits against illegal file sharing. However, the IFPI efforts were somewhat thwarted a month later when a Canadian judge ruled that downloading a song from an Internet file-sharing music site did not amount to infringement of copyright law. In 2006, nearly 2,000 lawsuits against illegal music downloads were served in 10 European countries, bringing the total number of cases initiated by the IFPI to 5,500. The 2006 lawsuits targeted individuals in Austria, Denmark, Finland, Germany, Iceland, Italy, Portugal, Sweden, and Switzerland. The suits mainly targeted users of peer-to-peer networks, including FastTrack, Gnutella, eDonkey, DirectConnect, BitTorrent, Limewire, WinMX, and SoulSeek.[24]

Another approach businesses have used to protect music copyrights involves **streaming**. Streaming refers to a customized, on-demand radio service. These are harder to pirate, because copies of the music are not downloaded and stored on users' hard drives, creating virtual libraries. Streaming provides music distributors with new revenues from selling subscriptions to the music for which they hold the copyright. The benefits of this were seen almost immediately. When a court ordered San Diego–based MP3.com to pay $10 million for creating a database of more than 45,000 CDs without copyright permission, the company agreed to a licensing fee. MP3.com agreed to pay 1.5 cents each time it copied a track of music and about 0.3 cents when a customer downloaded the song.[25]

Piracy of Movies on CDs and DVDs

With advances in technology, movies can be downloaded from the Internet to CDs or DVDs more easily than ever. The Motion Picture Association of America studied the problem and found that Hollywood studios alone lost $6.1 billion worldwide in 2005. In response to this costly epidemic, the Federal Communications Commission ordered that all U.S.-made digital television

receivers, by July 1, 2005, had to have technology installed meant to block the widespread and illegal redistribution of copyrighted programming.[26]

Some governments responded to entreaties by the motion picture industry. In 2004, a Hong Kong judge ruled that two managers at Golden Science Technology, a licensed disk-replication company in Hong Kong, had produced illegal copies of movies and other material. A raid of the Golden Science Technology warehouse seized 22.4 million disks, including 130,000 copies of the movie *Titanic*. The judge ordered both individuals to serve 6½ years in prison, the longest prison sentence to date for pirating movie disks.

Despite the effort shown by the Hong Kong courts, companies were increasingly worried about the spread of movie piracy, especially in Asia. Blockbuster, a U.S. movie rental chain, announced in 2005 that it was closing all of its 24 Hong Kong stores, because it could not compete against low-cost pirated DVDs and CDs readily available for sale throughout China and Hong Kong.[27]

In 2005, the United States stepped up its efforts to combat piracy, announcing an 11-nation crackdown on organizations responsible for stealing copies of the latest *Star Wars* film, worth more than $50 million. Four people were arrested, 8 major distribution centers were shut down, and hundreds of computers used to duplicate movies were seized. U.S. Attorney General Alberto Gonzalez said, "The Justice Department is striking at the top of the copyright piracy supply chain—a distribution chain that provides the vast majority of illegal digital content now available online." The U.S. Justice Department efforts were coordinated with law enforcement authorities from Australia, Belgium, Canada, Denmark, France, Germany, Israel, the Netherlands, Portugal, and the United Kingdom, indicating the widespread global reach of illegal piracy.

Managing Scientific Breakthroughs

Dramatic advances in the biological sciences also have propelled the impact of technology on our lives and business practices. As explained in Chapter 13, biotechnology refers to a technological application that uses biological systems or living organisms to make or modify products or processes for specific use. Recent unprecedented applications of biological science to industry have made possible new, improved methods of health care and agriculture, but they have also posed numerous ethical challenges regarding safety and the quality of life.

As Bill Joy of Sun Microsystems warns, speaking of biotechnology as well as other innovative applications of science, "21st century technologies . . . are so powerful that they can spawn whole new classes of accidents and abuses. Most dangerously, for the first time, these accidents and abuses are widely within the reach of individuals or small groups. They will not require large facilities or rare raw materials. Knowledge alone will enable the use of them."[28]

Human Genome

When Celera Genomics Group announced in 2000 that it had finished the first sequencing of a **human genome**, the achievement was hailed as the most significant scientific breakthrough since landing a man on the moon. Strands of human deoxyribonucleic acid, or DNA, are arrayed across 23 chromosomes in the nucleus of every human cell, forming a unique pattern for every human. These strands are composed of four chemical units, or letters, used over and over in varying sequences. These replicated letters total 3 billion and form the words, or

genes—our unique human signature—that instruct cells to manufacture the proteins that carry out all of the functions of human life. Scientists have also cracked the DNA for other species as well, including that of the malaria parasite, one of the world's biggest killers.[29] The identification of human genes is critical to the early diagnosis of life-threatening diseases, the invention of new ways to prevent illnesses, and the development of drug therapies to treat a person's unique genetic profile. A new era of medicine, as well as great opportunity for biotechnology companies, appeared to be born with the decoding of the human genome.

However, while advances in understanding DNA were exalted as one of the human race's greatest achievements, ethical challenges emerged in private and public research focusing on genetics.

> One family, who possessed a rare genetic heart disease called Brugada syndrome, wondered how others might react if they learned of the family's medical condition. Would employers want to hire someone who might die prematurely or require an expensive implantable defibrillator? Would they be eligible for individual health care coverage or be able to afford life insurance if their condition were known? The underlying fear for this family and others with genetic conditions was whether they would be treated fairly if their genetic fingerprints became public.

The debate over whether advances in human genome sequencing and genetic research outweigh the risks or harms will continue for years. What is clear is that our scientific understanding of the human body and its makeup has changed, and significant technological innovations are on the horizon. What is not clear is who, if anyone, can manage these changes to better ensure the improvement of the quality of our lives and society.

Biotechnology and Stem-Cell Research

Complementing the discovery of DNA sequencing were numerous medical breakthroughs in the area of regenerative medicine. **Tissue engineering**, the growth of tissue in a laboratory dish for experimental research, and **stem-cell research**, research on nonspecialized cells that have the capacity to self-renew and to differentiate into more mature cells, were two such breakthroughs. Both offered the promise that failing human organs and aging cells could be rejuvenated or replaced with healthy cells or tissues grown anew. While the promise of immortality may be overstated, regenerative medicine provided a revolutionary technological breakthrough for the field of medicine.

Stem-cell research spilled over from the laboratories into government arenas as politicians weighed in on the ethical controversy. A 2006 Gallup poll reported that 61 percent of the U.S. public believed stem-cell research was morally acceptable. Support for stem-cell research was evident in California, where nearly 60 percent of voters in 2004 supported Proposition 71, which set aside $350 million annually for a decade or a total of more than $3 billion. This amount dwarfed the $25 million the National Institutes of Health allocated to embryonic stem-cell research in 2004. The European Parliament encouraged the financial units of the EU nations to free up nearly $5 billion in research to be used specifically to study the potential windfall of medical advances reaped from stem-cell research.[30] Exhibit 14.B discusses various countries' controls, or lack of controls, for stem-cell research.

Supported by private and government funding, hundreds of biotechnology companies and university laboratories answered the call and developed new ways to replace or regenerate failed body parts. Research included efforts to insert bone-growth factors or stem cells into a porous material cut to a specific shape, creating

new jaws or limbs. Genetically engineered proteins were successfully used to regrow blood vessels that might repair or replace heart values, arteries, and veins. The process to regrow cartilage was used to grow a new chest for a boy, and a human ear was grown on a mouse.

In addition, the Food and Drug Administration (FDA) laid the early groundwork for generic versions of biotechnology medicines, an effort that could transform the market for some of the most innovative and expensive new treatments for cancer and other diseases. This effort was particularly important as some of the oldest biotech drugs, such as Eli Lilly's bioengineered insulin Humulin and Genetech's Nutropin growth hormone, were about to lose patent protection. "We are concerned about finding safe ways to lower drug costs for Americans," said FDA Commissioner Mark McClellan. "If we can find a safe plan to produce generic or follow-up products for biologics, that can be an important step." According to medical drug market experts, the market for such drugs is more than $22 billion annually.[31]

Cloning

In 1986, a Danish scientist announced the first successful cloning of a sheep from fetal cells. Shortly thereafter a University of Wisconsin scientist succeeded with cows. Ten years later, in 1996, the Roslin Institute in Scotland announced it had cloned healthy calves from fetal cells. Another significant breakthrough occurred in 1997, when Ian Wilmut of the Roslin Institute unveiled Dolly, the first mammal to be cloned from adult cells. A year later, scientists from the University of Massachusetts reported that they had discovered a method of cloning cows with a process that was simpler and more efficient than Wilmut's method. In 2003 doctors in China reported they had become the first to make an infertile woman pregnant with an experimental technique devised in the United States for women who have healthy genes but defects in their eggs that prevent embryos from developing. Critics argued that this technique is perilously close to human cloning.[32]

Bogus reports of human cloning appeared in 2002, based on a publicity stunt by the Clonaid organization, a religious movement intent on cloning its leaders. Two years later, technology appeared to have taken another step forward when scientists in South Korea reported they had created human embryos through cloning and extracted embryonic stem cells. This work made possible the birth of a cloned human baby even more feasible. The validity of this research was questioned when subsequent research by the same South Korean scientists was found to be without merit, as discussed in Exhibit 14.C. Nonetheless, medical advances toward human cloning were appearing.[33]

As each new announcement of a more advanced and successful cloning experiment was announced to the public, more fears arose. Whether it was a vision of Jurassic Park dinosaurs running loose in a metropolitan downtown area or the eerie absurdity of cloning multiple Adolf Hitlers in the film *The Boys of Brazil*, fears of cloning living tissue invaded our lives. In 2002, the U.S. Senate began debates on a bill to ban human cloning, although its sponsors anticipated a long and difficult battle. Organizations in support of human cloning and against the U.S. government's proposed restrictions were formed and Web sites were created, such as that of the Human Cloning Foundation. Both those supporting and opposing cloning have been vehement in making their stances known to the public in the hopes of influencing politicians. By 2005, an overwhelming majority of Americans surveyed supported embryonic stem-cell research. "Regardless of party identification or religious affiliation, most adults believe embryonic stem-cell research should be allowed . . . as nearly three-quarters (74 percent) of U.S. adults believe stem-cell research should be allowed today (73 percent in 2004)."[34]

In 1997, when Dolly appeared on the cloning scene, there were no laws on record that prevented scientists from attempting human cloning. Experts recognized that the technique used in Scotland to clone a sheep was so simple and required so little high-tech equipment that most biology laboratories with a budget of a few hundred thousand dollars could attempt it.

In 2003 the United Nations General Assembly considered three proposals aimed at human cloning. One proposal, pushed strongly by the United States, was backed by more than 60 countries and called for a ban of all forms of cloning, both reproductive cloning (to produce a baby identical to its genetic parents) and therapeutic cloning (for medical purposes). A more moderate proposal was sponsored by Belgium and backed by 20 countries, including Britain, Japan, and China. This proposal suggested that only reproductive cloning would be banned and the fate of therapeutic cloning would be left up to individual nations. Finally, a third proposal, championed by many Islamic nations, argued that the issue should be deferred for two years. By a one vote margin, the United Nations put off for two years any international ban on human cloning.[35]

With little guidance at the international level, national organizations sought to establish ethical rules regarding cloning practices. In 2005, the United States National Academy of Sciences issued guidelines for embryonic stem-cell research, seeking to provide a clear path through the ethical minefield. The guidelines outlawed some far-reaching endeavors; for example, scientists could not insert embryonic stem cells into a human embryo. They also could not introduce stem cells into apes or monkeys, avoiding the nightmarish possibility that an animal could give birth to a human or develop a human mind. Otherwise, most stem-cell research was permitted. The guidelines were voluntary but the organization hoped that most institutions, state stem-cell programs, scientific journals, and organizations offering research grants would adhere to the suggested behavior.

In the aftermath of the South Korean cloning fraud, discussed in Exhibit 14.C, the International Society for Stem Cell Research (ISSCR) agreed to convene a task force of experts from a dozen countries, including Japan, Korea, the United Kingdom, and the United States, in 2007 to discuss what guidelines might be formulated. "The [South Korean] scandal created a general consensus among scientists that bioengineering must stand on firm ethical grounds, which is why the guidelines will have great symbolic meaning," said Professor Kim Dong-wook of Yonsei University.[36]

Clearly stem-cell research leading to the possibility of human cloning is an important issue and will likely increase in prominence in the near future. What must also be clear is the need for specific and binding ethical guidelines for scientists engaging in this volatile field to protect society. The debate over how to govern this scientific community and its work inevitably will continue for years.

Bioterrorism

An emerging yet tragic outcome of scientific breakthroughs in bioengineering is the potential for **bioterrorism**. Terrorist groups see the use of deadly bioengineered diseases and poisons, such as smallpox, anthrax, and bubonic plague, as effective tools since they are more difficult to detect when transported than guns or bombs. Germs are more effective as a terrorist tool because tens of thousands of people easily can be affected. Oklahoma Governor Frank Keating said, "It not only stunned me how horrific a biological attack could be, but also how woefully unprepared we are."[37]

President Bush announced in 2003 Project BioShield, a $5.6 billion, 10-year government program to spur pharmaceutical companies to develop vaccines and antidotes to combat bioterrorism. Yet three years after the announcement, bioterrorism experts claimed that nothing had been done, and the major pharmaceutical companies have waited months, if not years, for government agencies to act.[38]

One company did see an opportunity to become a "biodefense contractor," as it developed a pharmaceutical-defense system, and suffered public scrutiny. Bayer Corporation was in the public hot seat after the 2001 anthrax scare in the United States. The company possessed large quantities of Cipro, an anti-anthrax drug for which it held the patent. When Bayer attempted to sell Cipro, the public was appalled that a company would try to profit from a country's bioterrorism disaster. Bayer President Helge Wehmeier argued, "I haven't heard of anyone giving their bombers away because America is in need."[39]

Genetically Engineered Foods

The biotechnological revolution targeting improvements in health care was also adapted for use by the agricultural industry. Technological advances in genetics and biology led to an unprecedented number of innovations. **Genetic engineering**, altering the natural makeup of a living organism, allowed scientists to insert virtually any gene into a plant and create a new crop or a new species. The economic force of this technological revolution was immediately apparent. Venture capitalists injected $750 million into the agricultural industry, an area generally ignored by venture capitalists throughout the 1980s.

Schools of salmon and trout were engineered to grow twice as fast as before. Soybeans, cotton, corn, and other crops were genetically engineered to resist pests or to be impervious to herbicides used to control weeds. Some were altered to yield a higher nutritional value. Cows, sheep, and goats were treated to produce drugs in their milk. "We are starting the century of biology," announced J. Craig Venter, president of the Institute for Genomic Research. The payoff potential was huge.[40]

In Europe, a severe backlash emerged to **genetically modified foods**, or GM foods, that is, food processed from genetically engineered crops. Protesters there called GM foods "Frankenstein foods." Heinz Corporation, a U.S.-based food producer, announced that it would not sell GM foods in Europe. Similarly, Bayer CropScience, a unit of Bayer AG of Germany, decided against selling gene-altered seeds in Britain, despite winning landmark regulatory approval.

> By 2003, opposition to GM food was widespread. In France, 89 percent said it was bad to scientifically alter fruits and vegetables "because it could hurt human health and the environment." In Germany, 81 percent of those surveyed opposed GM foods; in Japan, 76 percent; and in Italy, 74 percent. Although opposition in the United States was less widespread, 55 percent of Americans also believed genetically modified foods were a bad idea.[41]

Despite this public opposition, some firms knew that GM foods were an important scientific breakthrough and an attractive financial investment. One such firm was Monsanto.

> In 1998, Monsanto Company became the first company to genetically engineer corn to resist rootworm, an insect that caused $1 billion in damages annually to the largest U.S. crop. The company reported that farmers would no longer have to spend $150 million annually on chemicals to control rootworm, which infested about 15 million acres. Five years after Monsanto's initial announcement Monsanto received clearance from the U.S. Environmental Protection Agency to begin to sell the first corn plant genetically modified to resist the rootworm insect.[42]

Other genetically modified products were introduced with mixed results. The food industry generally shunned bioengineered seeds to grow sugar beet plants, the source for sugar for food and candy manufacturers. But genetically modified tobacco, which contained virtually no nicotine, was welcomed by the Leggett

Group, a discount-cigarette maker that targeted low-income people who were trying to quit smoking.

By 2004, the opposition to GM foods began to weaken in Europe. Britain allowed farmers to grow a strain of biotech corn for cultivation purposes and to feed dairy cows, but retained the ban on GM sugar beets. Shortly thereafter, the European Union approved the manufacture of a genetically engineered corn, ending a six-year moratorium on approvals for biotechnology crops that led to a bitter trade dispute with the United States. Then, in 2006, the World Trade Organization (WTO) ruled that the European Union (EU) had breached international rules by restricting imports of genetically modified crops and food made from them. While bioengineering experts did not feel that the WTO ruling would flood Europe with GM products, they did believe that it would discourage other countries from adopting barriers similar to those developed by the EU and would set a precedent that countries must have sound scientific reasons for rejecting genetically modified crops. "One reason we brought the case was because of the chilling effect the EU's actions had on the adoption of biotechnology," said a United States trade official.[43]

In other countries genetically modified food was welcomed. Russia embraced this new technology, as did China.

> After losing the battle to insects and finding that pesticides often were ineffective on the North China Plain, where cotton was the primary crop, cotton growing began to flourish again. "I was the first one in the village to plant these new [bioengineered] cotton seeds, but when everyone saw how great the results were, they started growing again, too," said An Deyin, a Chinese farmer.

China's leaders made genetic research a top scientific priority, funneling billions of government dollars into research on modifying the genes of crops and vegetables. Government leaders saw genetic crop production as a source of stable food supplies and the path to a national presence in the agricultural import-export arena. By 2000, 1.2 million to 2.4 million acres of biotech crops had been planted in China. Professor Zhangliang Chen estimated that within 5 to 10 years, half of the country's fields would be planted with GM rice, potatoes, and other crops. While predictions of widespread planting of GM crops in China were common, most countries, including China, have been slow to join the GM-food campaign strongly adopted in the United States, as shown in Figure 14.3.

The controversies over genetic engineering, stem-cell research, cloning, and genetically modified food production raise serious ethical and social issues. The questions concerning the role of businesses, social activist groups, or governments in overseeing these technological developments must continue to be addressed, as new innovations appear on the horizon.

- Businesses have addressed many privacy issues at work and in e-commerce by developing privacy policies and by sharing information and technology through voluntary industry initiatives.
- Acts of sabotage by computer hackers threaten companies' control of information, causing businesses to develop elaborate information security systems to more quickly detect hacking efforts and to patch systems targeted by viruses or worms.
- Businesses have entrusted the management of technology to their chief information or privacy officers. For issues that go beyond the business organization and affect society in general, it is unclear whether businesses,

social groups, or governments—or some combination of these—should manage technology and its change.

- Company and industry initiatives have been joined by governmental action to better shield children from the growing and lucrative Internet pornography industry.
- Threats of software, music, and movie piracy challenge businesses' ownership of their property, calling for industry and international governmental responses to these ethical violations.
- Fears associated with human genetic research, stem-cell research, human cloning, and genetically modified foods have raised objections from social activist and consumer groups. Businesses have attempted to address these fears and dispel false concerns, while seeking to promote the benefits of scientific technological breakthroughs.

Discussion Case: *We're Simply Downloading Music—So What's the Big Deal?*

Jose is a junior in college and he loves music. It helps define who he is, and he enjoys showing off the new tunes he has downloaded to his friends, especially Rachel, whom he is trying to impress. His music helps him study, relax, and meet new people. But his friend Rachel has just told him that she has received a letter from some music group (the Recording Industry Association of America) telling her that she will be sued if she does not stop downloading music. She is frightened and confused by the letter, and now Jose is concerned too.

Jose and Rachel are caught in the middle of an ethical and legal controversy over the protection of copyrighted music. What are the rights of the musicians who created the music and the companies that recorded and distributed it? What are the rights of music fans to use readily available software to download music from the Internet and store it to play later at their pleasure?

The Recording Industry Association of America (RIAA) took an exceptionally hard stance in early 2003 when it filed 261 lawsuits, charging Internet music downloaders with copyright infringement. With recorded music sales down 26 percent in four years, industry officials believed that the only way to stem the widespread file swapping was to make people realize that they would be punished for participating.

The RIAA continued its battle in 2003 and 2004 by suing several hundred individuals for illegally downloading and distributing copyrighted music over the Internet. One RIAA letter stated, "The purpose of this notice is to provide you with the opportunity to resolve this matter and avoid being sued." RIAA alleged that individuals were using Internet services such as Kazaa and Grokster to access, download, and store music. In one action, it specifically targeted subscribers of five Internet service providers based along the East Coast.

Later in 2004, the RIAA turned to universities in its quest to stop illegal file sharing of music. This time, it targeted college students and others who had allegedly used networks at 21 different universities to illegally share music files. Commented the provost of the University of Michigan, "We will of course comply with the law. Violation of copyright laws is a violation of our own computing policies. We emphasize the proper-use policy and we have had programs to discuss this issue."

But the RIAA legal onslaught was not over. A year later in April 2005, university students at 18 colleges with access to the Internet2 network were served with federal lawsuits. Internet2 is used by several million university students, researchers, and professors around the world but is generally inaccessible to the

public. The RIAA accused students of sharing an average of 2,300 songs each. RIAA reported that it found evidence of more illegal file sharing at 140 more schools in 41 states and sent warning letters to university presidents threatening additional legal action if steps were not taken to stop this illegal epidemic.

When Jose learned about this latest action, he become increasingly concerned, since he knew that he and his friends, including Rachel, had all used the Internet2 system at their school to download music.

Jose decided he needed more information, so he went to his blog and began discussing this issue with people he had met through the Internet. Mike, who was a student at Penn State, told Jose that his school provided him and his friends with a legal method to download music from a catalog of half a million songs. According to Mike, Penn State had entered into a deal with Napster. After losing a major legal battle with RIAA in 2003, Napster had developed a new service that allowed him to listen to an unlimited number of songs as often as he wanted, as long as he remained a student at Penn State. And when he graduated, Mike said, he could burn his tunes to a CD and pay only 99 cents per song. Mike heard this was possible because of the $160 information technology fee every student paid each year.

Now Jose was really confused. Why would Rachel get this threatening letter for downloading music, but Mike said it was OK and legal to do this at Penn State? Another blogger, Jasmine, who was a student where Jose and Rachel went to school, posted the letter that the university circulated at student orientation informing students that the school had a strict policy against students illegally downloading songs. If discovered, the student could face disciplinary action, even dismissal from school. When Jose told Rachel about their school's policy, they were really scared since their parents would be very angry if either were dismissed from school for something their parents would view as so silly as downloading music.

Jose and Rachel weren't sure what to do. Should they delete all of their songs, in fear of action that could be taken by the RIAA, their university, or even worse, their parents? Or should they just go along as normal, downloading the songs they liked and enjoyed listening to when studying, relaxing, and with friends? Surely the RIAA couldn't know about their actions. They only downloaded a couple of hundred songs, not thousands as RIAA claimed students had done in their recent round of lawsuits. Maybe no one would ever know.

Sources: "261 Lawsuits Filed on Internet Music Sharing," *The New York Times Online,* September 9, 2003, *www.nytimes.com;* "Music Industry Sends Warnings on Alleged Piracy," *The Wall Street Journal,* October 20, 2003, p. B9; "Record Industry Files 532 Suits against Music Downloaders," *The New York Times Online,* January 21, 2004, *www.nytimes.com*; "Music Group Files Another File-Sharing Suit," *The Wall Street Journal,* February 18, 2004, p. B10; "RIAA Sues People at 21 Colleges, Claiming Illegal Music Sharing," *The Wall Street Journal,* March 24, 2004, p. B4; "RIAA to Sue Internet2 Users," *The Wall Street Journal Online,* April 12, 2005, *online.wsj.com;* and "Penn State Will Pay to Allow Students to Download Music," *The New York Times Online,* November 7, 2003, *www.nytimes.com*.

[1] "Cyber-Crime Issues Escalate Worldwide," Institute for Global Ethics, *Ethics Newsline*, February 27, 2006, *www.globalethics.org.*

[2] Bill Joy, "Why the Future Doesn't Need Us," *Wired*, April 2000, *www.wired.com/wired/archive/8.04/joy.*

FIGURE 14.1 Consumer Perceptions of Online Privacy

Source: Data taken from "Americans and Online Privacy: The System Is Broken," Annenberg Public Policy Center at the University of Pennsylvania, 2003, *www.asc.upenn.edu.*

Percentage of Home Internet Users Who:

Knew Web sites collected information about them even if they

Incorrectly believed that a Web site with a privacy policy would not share their personal information	57
Thought that Web site privacy policies were easy to understand	47
Have searched for information on how to protect their personal data	46

Have used filters to block spam	43
Have used software that looks for spyware	23
Have used software that hid their computer's identity from Web sites	17

[3] "Germany's Hunt for Terrorists Hit Unlikely Obstacle," *The Wall Street Journal*, August 9, 2002, pp. A1, A7; and "Hurdle for U.S. in Getting Data on Passengers," *The New York Times Online,* May 31, 2006, *www.nytimes.com.*

[4] For an excellent discussion of the ethical issues surrounding RFID technology, see Alan R. Peslak, "An Ethical Exploration of Privacy and Radio Frequency Identification," *Journal of Business Ethics* 59 (2005), pp. 327–45.

[5] "Privacy: Don't Ask Technology to Do the Job," *BusinessWeek*, June 26, 2000, p. 52.

[6] "Tech Alliance to Share Data about Hackers," *The Wall Street Journal*, January 16, 2001, pp. A3, A4.

[7] "U.S. in Tentative Pact Protecting Europeans' Privacy," *The Wall Street Journal*, February 20, 2000, p. B6; and "Europe's New High-Tech Role: Playing Privacy Cop to the World," *The Wall Street Journal*, October 10, 2003, pp. A1, A16.

[8] For a discussion of Internet regulation see Norman E. Bowie and Karim Jamal, "Privacy Rights of the Internet: Self-regulation or Government Regulation," *Business Ethics Quarterly* 16, no. 3 (2006), pp. 323–42.

[9] "Time Warner Alerts Staff to Lost Data," *The Wall Street Journal Online,* May 3, 2005, *online.wsj.com;* "Citigroup Says Data Lost On 3.9 Million Customers," *The Wall Street Journal Online,* June 6, 2005, *online.wsj.com;* and "MasterCard Says 40 Million Files Are Put at Risk," *The New York Times Online,* June 18, 2005, *www.nytimes.com.*

[10] "Computer 'Worm' Widely Attacks Windows Versions," *The New York Times*, August 13, 2003, *www.nytimes.com.*

FIGURE 14.2 The Worms Are Getting Faster

Source: Foundstone, Inc., *www.foundstone.com.*

Name of Worm		Alert Received	Work Released	Number of Days to Patch or Prevent	
Melissa		December 1, 1999	March 27, 1999	65	
(i)	Sadmind	December 29, 1999	May 8, 2001	496	
(ii)	Sonic	July 18, 2000	October 30, 2000	104	
(iii)	Bugbear	March 29, 2001	September 30, 2002	550	
(iv)	Code Red	June 18, 2001	July 19, 2001	31	
(v)	Nimda	August 15, 2001	September 18, 2001	34	
(vi)	Spida	April 17, 2002	May 21, 2002	34	
(vii)	SQL Slammer	July 24, 2002	January 25, 2003	185	
(viii)	Slapper	July 30, 2002	September 14, 2002	46	
(ix)	Blaster/Welchia/Nachi		July 16, 2003	August 11, 2003	26
(x)	Witty	March 18, 2004	March 20, 2004	2	
Sasser		April 13, 2004	April 30, 2004	17	

[11] "Computer Viruses Still Proliferating; E-Mail Risk Rising," *The Wall Street Journal*, March 4, 2002, p. B5.

On March 2, 2005, about 150 business school applicants took advantage of a 10-hour security vulnerability on a site maintained by ApplyYourself, Inc., a Virginia-based company that manages admissions data for dozens of elite business schools. A hacker was able to post instructions to a bulletin board belonging to a *BusinessWeek* online forum enabling individuals to access their own admissions files. Since most of the schools had not made final admissions decisions on the applicants, the individuals saw only preliminary evaluations or data and some accessed only blank screens.

Nonetheless, many of the universities affected took the breach of security very seriously. "This behavior is unethical at best—a serious breach of trust that cannot be countered by rationalization," said Kim Clark, dean of the Harvard Business School. Most schools—including Carnegie Mellon, Harvard, Duke, and

MIT—decided to deny admission to the prospective students who had accessed the ApplyYourself site. Stanford officials decided to review each hacker's case individually before making a final decision, but added, "Our mission statement talks about principled, innovative leaders and we take the principled part seriously."

A few days after the incident occurred, Dartmouth broke ranks from the other universities and announced that it would admit some of the 17 business school applicants who had hacked into its computerized database. After lengthy discussions among Dartmouth faculty and staff, the university decided that the action should be a major strike against the prospective students but was not enough, by itself, to disqualify them. Dartmouth's dean, Paul Danos, said, "Their curiosity got the best of them. All of them expressed some remorse. Some were admitted. Some were rejected."

Sources: "Business Schools Bar Applicants Who Hacked Admissions Web site," Institute for Global Ethics, *Ethics Newsline,* March 14, 2005, *www.globalethics.org;* and "Dartmouth Swims against Tide, Will Admit Some of Hackers," *Pittsburgh Post-Gazette,* March 18, 2005, p. B6.

[12] 2005 Global Business Security Index Report, International Business Machines, *www.ibm.com.*

[13] "Around the World, Hackers Get Stuck in 'Honeypots,'" *The Wall Street Journal*, December 19, 2000, p. A18; and see Spitzner's Web site at *http://project.honeynet.org.*

[14] "From Black Market to Free Market," *BusinessWeek,* August 22/29, 2005, pp. 28–32.

[15] Edward Prewitt and Lorraine Cosgrove Ware, "The State of the CIO '06: A Report," *CIO Research,* at *www.cio.com/state;* and "From Gearhead to Grand High Pooh-Bah," *BusinessWeek*, August 28, 2000, pp. 129–30. Also see "Focus On: The Chief Information Officer," *BusinessWeek*, December 16, 2002, pp. 24–25; and "Chief Privacy Officers: Real Change or Window Dressing," *Business Ethics*, September–October 2001, pp. 8–9.

[16] Jerry Ropelato, "Pornography Industry Revenue Statistics," 2006, *www.TopTenREVIEWS.com*.

[17] "Police Raid Yahoo! Japan Office in Pornography Probe," *The Wall Street Journal*, November 28, 2000, p. A23; "Yahoo! Ordered to Bar the French from Nazi Items," *The Wall Street Journal*, November 21, 2000, pp. B1, B4; and "Yahoo! Plans to Remove Adult Content," *The Wall Street Journal*, April 16, 2001, p. B6.

[18] See GetNetWise's Web site at *www.GetNetWise.org.*

[19] "Public Libraries Must Use Internet Filters, Supreme Court Rules," Institute for Global Ethics, *Ethics Newsline*, June 30, 2003, *www.globalethics.org.*

[20] "Software Piracy Still Costs Billions," *Knight Ridder Tribune Business News,* June 5, 2006, p. 1.

[21] "China Begins Effort to Curb Piracy of Computer Software," *The New York Times Online,* May 30, 2006, *www.nytimes.com.*

[22] "Sega Closes 185 Web Sites to Fight Software Piracy," *The Wall Street Journal*, July 21, 2000, p. B5.

[23] "Free Downloads—After this Message," *BusinessWeek*, October 9, 2006, p. 95; "U.S. Is Only the Tip of Pirated Music Iceberg," *The New York Times*, September 26, 2003, *www.nytimes.com;* and "One-Third of Music CDs Sold In the World Are Pirated," *The Wall Street Journal Online,* June 23, 2005, *online.wsj.com.*

[24] "Music Industry's Assault on Piracy Goes Outside U.S.," *The Wall Street Journal,* March 31, 2004, p. B3; "Canadian Ruling on File Sharing Sends Shock Waves through Music Industry," Institute for Global Ethics, *Ethics Newsline,* April 5, 2004, www.globalethics.org; and "Music Industry Files More Suits In Europe," *The Wall Street Journal Online,* April 4, 2006, *online.wsj.com.*

[25] "If You Can't Lick 'Em, License 'Em," *BusinessWeek,* June 26, 2000, p. 46.

[26] "Estimates of Copyright Piracy Losses Vary Widely," *The Wall Street Journal Online,* June 2, 2006, *online.wsj.com;* and "FCC Acts to Protect Digital Content," *The Wall Street Journal,* November 5, 2003, p. A7.

[27] "Blockbuster to Close All Stores In Hong Kong by Mid-2005," *The Wall Street Journal,* February 2, 2004, p. B3.

[28] Joy, "Why the Future Doesn't Need Us."

[29] "Genetic Secrets of Malaria Bug Cracked at Last," *The Wall Street Journal*, January 18, 2002, pp. B1, B6.

Government controls, or lack of controls, regarding scientific stem-cell research varies from country to country. In some countries, the controls apply only to specific types of research, while in other countries there is little control of scientific research in this field.

Germany: The Embryo Protection Law forbids all human embryonic stem-cell research, but research is permitted on legally imported cells, and public funding is available for animal and adult embryonic stem-cell research.

Britain: Human stem-cell research is permitted for therapeutic purposes, using embryos left over from fertility treatments. Cloning of embryos for therapeutic research has been permitted since 1990.

Sweden: Ten percent of the total human embryonic stem-cell lines in existence by 2001 were created in this country. Research is allowed on embryos left over from fertility treatments.

France: Guidelines were developed that permit human embryonic research for stem cells but cloning of stem cells has been banned since the 1994 Bioethics Law was passed.

Israel: No formal laws and little public opposition to stem-cell research exists. Researchers at two universities created four stem-cell lines, and research is expanding.

Japan: This nation is considering rules to allow research on human embryos left over from fertility treatments. Human cloning has been banned since 2000 and is punishable with up to 10 years in jail and fines of $90,000.

Singapore: Ethical guidelines were introduced in 2002. Researchers at the National University of Singapore created six stem-cell lines that were commercially available.

Sources: Information taken from “At Risk: A Golden Opportunity in Biotech,” *BusinessWeek*, September 10, 2001, pp. 85–87; and “Stem-Cell Research Is Forging Ahead in Europe,” *The Wall Street Journal*, July 13, 2001, pp. B1, B4.

[30] “Bush to Allow Funds for Study of Stem Cells,” *The Wall Street Journal*, August 10, 2001, pp. A3, A4; “California Vote Brings Windfall for Stem Cells,” *The Wall Street Journal,* November 4, 2004, pp. B1, B7; and “European Parliament Urges Resumption of Stem-Cell Research,” Institute for Global Ethics, *Ethics Newsline,* November 24, 2003, *www.globalethics.org.*

[31] “FDA Takes Steps toward Allowing Generic Versions of Biotech Drugs,” *The Wall Street Journal*, February 18, 2004, pp. A1, A6.

[32] “Pregnancy Created Using Infertile Woman’s Egg Nucleus,” *The New York Times Online,* October 14, 2003, *www.nytimes.com.*

[33] The ethical debate over cloning was fueled by the reported medical achievements involving humans. For a thorough discussion of these ethical arguments see Rushworth M. Kidder, “The Ethics of Cloning,” *Ethics Newsline,* February 17, 2004, *www.globalethics.org.* Also see Arlene Weintraub, “What’s Ethical and What Isn’t,” *BusinessWeek,* January 16, 2006, p. 76.

[34] “Public Support for Stem-Cell Research Remains High,” Institute for Global Ethics, *Ethics Newsline,* June 13, 2005, *www.globalethiucs.com.* Also see *www.humancloning.org.*

In May 2005, researcher Hwang Woo Suk of South Korea’s Seoul National University shocked the world when he reported that his team of 24 scientists had used cloning to transform skin samples taken from 11 sick or injured people into supplies of embryonic stem cells. The scientific report appeared in the journal *Science* and marked a significant leap for therapeutic cloning, a proposed means of generating supplies of nerves, heart muscle, or other cells perfectly matched to particular patients.

Despite fears over the increasing possibility of human cloning, Hwang cautioned, “Our proposal is limited to finding a way to cure cancer. That is our proposal and research goal.” Supporters of Hwang’s research heralded the achievement as a “really major milestone because it puts the whole technique on the map.”

Six months later, it became clear that Hwang had fabricated the evidence for all of the research published in the journal article, according to a report issued by the Seoul National University panel that investigated Hwang’s work. The panel’s findings stripped any possibility of a legitimate achievement in human cell cloning, disgracing a researcher who promised to make paralyzed people walk and whose features had been engraved on a Korean postage stamp.

London’s *Financial Times* noted that the fraud caused thunderous repercussions in the scientific world, not only for research institutions and patients, who hoped that the new techniques could cure their illnesses, but also for the scientific process itself. Critics said the peer review system broke down and the journal publishing the findings was sloppy in its review since it wanted to rush newsworthy results into print.

Despite the report from his own university saying that his work was fabricated, Hwang stood by his research saying that he has the technology to produce tailored embryonic stem cells and can reproduce the process at any time.

Sources: “Seoul Team Creates Custom Stem Cells From Cloned Embryos,” *The Wall Street Journal Online,* May 20, 2005, *online.wsj.com;* “Researcher Faked Evidence of Human Cloning, Koreans Report,” *The New York Times Online,* January 10, 2006, *www.nytimes.com;* and “Blatant Fraud Suspected in South Korean Stem Cell Research,” Institute for Global Ethics, *Ethics Newsline,* January 2, 2006, *www.globalethics.com.*

[35] “A Fight at the U.N. over Cloning,” *The New York Times Online,* November 5, 2003, *www.nytimes.com;* and “U.N. Puts Off Human-Clone Ban amid Demands by U.S., Vatican,” *The Wall Street Journal,* November 7, 2003, pp. A3, A8.

[36] “Task Force to Create Ethical Guidelines for Stem Cell Research,” Institute for Global Ethics, *Ethics Newsline,* January 16, 2006, *www.globalethics.org*.

[37] “The Next Phase: Bioterrorism?” *BusinessWeek*, October 1, 2001, pp. 58–61.

[38] “Nation Unready for Germ Attacks; Bioterror Defense Lags Despite 4 Years, $20 Billion,” *USA Today,* August 1, 2005, p. A1; and “Bid to Stockpile Bioterror Drugs Stymied by Setback,” *The New York Times Online,* September 18, 2006, *www.nytimes.com.*

[39] “Drug Companies Contemplate New Role as ‘Biodefense Contractors,’” *The Wall Street Journal*, November 12, 2001, pp. B1, B8.

[40] "We Are Now Starting the Century of Biology," *BusinessWeek*, August 31, 1998, pp. 86–87.

[41] "Broad Opposition to Genetically Modified Foods," Institute for Global Ethics, *Ethics Newsline*, July 7, 2003, *www.globalethics.org.*

[42] "Monsanto Falls Flat Trying to Sell Europe on Bioengineered Food," *The Wall Street Journal*, May 11, 1999, pp. A1, A10; and "Monsanto Wins EPA Clearance to Market Pest-Resistant Corn," *The Wall Street Journal*, February 26, 2003, p. D4.

FIGURE 14.3

Commitment to Biotechnology Crop Planting by Country

Source: International Service for the Acquisition of Agri-biotech Applications, reported in "Thai Chew Over Biotech Food," *The Wall Street Journal*, October 29, 2004, p. A13.

Country	Millions of Acres, 2003
United States	105.7
Argentina	34.3
Canada	10.9
Brazil	7.4
China	6.9
South Africa	0.9
Australia	0.25
India	0.25
Romania	Less than 0.25
Uruguay	Less than 0.25

[43] "World Trade Agency Rules for U.S. in Biotech Dispute," *The New York Times Online,* February 8, 2006, *www.nytimes.com.*

Key Terms

bioterrorism, *313*
chief information officer (CIO), *304*
computer hackers, *302*
Digital Millennium Copyright Act, *306*
genetically modified foods, *314*
genetic engineering, *314*
human genome, *309*
intellectual property, *305*
privacy policy, *298*
software piracy, *305*
stem-cell research, *309*
streaming, *307*
tissue engineering, *309*

www.privacyalliance.com	Online Privacy Alliance
www.truste.org	TRUSTe
www.bsa.org	Business Software Alliance
www.doegenomes.org	Human Genome Project
www.nlm.nih.gov/medlineplus/cloning and The National Institutes of Health	-Medline Plus—Cloning, U.S. National Library of Medicine
www.monsanto.com/biotech-gmo	Monsanto's biotechnology Web page

Internet Resources

Discussion Questions

1. Was it appropriate for the RIAA to repeatedly file lawsuits against those who were downloading music? If not, what else could the association have done to stem declining industry sales, which were partially due to free file-swapping of music?

2. Since other information and entertainment are available for free off the Internet, should music be available at no charge as well? Or, is it simply wrong to download copyrighted music?
3. Where do you draw the line permitting free information off the Internet, but try to respect the artists' intellectual property and rights to royalties from their creations?
4. As long as technology enables people to download music with greater anonymity, should people continue to download music files until they are caught?